PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-069830
(43)Date of publication of application : 11.03.1997

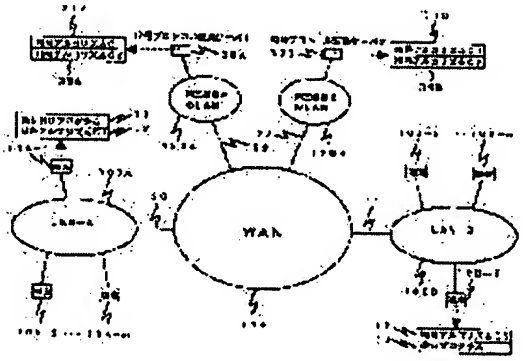
(51)Int.Cl. H04L 9/14
G09C 1/00

(21)Application number : 07-221928
(22)Date of filing : 30.08.1995

(71)Applicant : HITACHI LTD
(72)Inventor : NANBA DEN
TAKARAGI KAZUO
MIYAZAKI SATOSHI

(54) CIPHER COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To safely perform cipher translating processing when performing cipher communication between terminals to use mutually different ciphers.
SOLUTION: When transmitting data to a terminal 10B-1 connected to a LAN-B to use a cipher algorithm C1, a terminal 10A-1 connected to a LAN-A to use a cipher algorithm C1 generates two pieces of data, for which it is difficult to discriminate semantics, from the data to be transmitted. Then, two pieces of generated data are ciphered by using C1 and transmitted while being distributed to two cipher protocol translation servers 1 and 2. The cipher protocol translation servers 1 and 2 decode the data transmitted from the terminal 10A-1 by using C1 while sharing the processing with each other, perform cipher translating processing for reciphering the data by using C2 and then transmit the data to the terminal 10B-1. The terminal 10B-1 decodes the original transmit data from two pieces of data respectively transmitted from the cipher protocol translation servers 1 and 2.



LEGAL STATUS

[Date of request for examination] 07.02.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－69830

(43)公開日　平成９年(1997)３月11日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/14			Ｈ０４Ｌ	9/00	６４１
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ｅ

審査請求　未請求　請求項の数11　ＯＬ　（全 22 頁）

(21)出願番号　特願平7－221928

(22)出願日　平成７年(1995)８月30日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　難波　竜
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

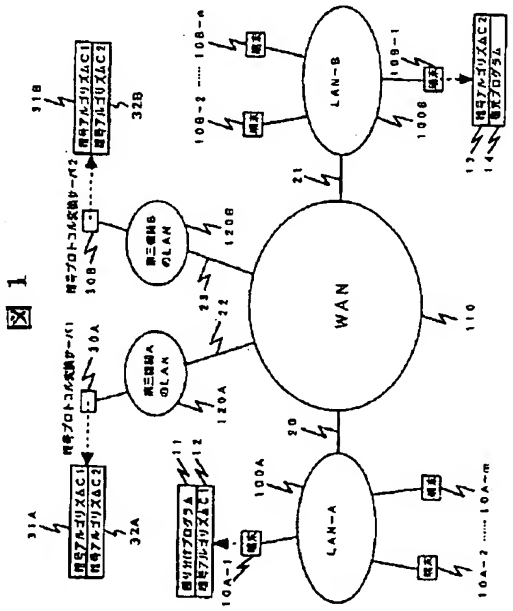
(72)発明者　宮崎　聡
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　富田　和子

(54)【発明の名称】　暗号通信システム

(57)【要約】
【目的】互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、安全に行うことが可能な暗号通信システムを提供する。
【構成】暗号アルゴリズムＣ１を使用するＬＡＮ－Ａに接続された端末１０Ａ－１は、暗号アルゴリズムＣ２を使用するＬＡＮ－Ｂに接続された端末１０Ｂ－１にデータを送信する場合に、送信すべきデータから意味判別困難な２個のデータを生成し、生成した２個のデータを、Ｃ１を使用して暗号化した後、２個の暗号プロトコル変換サーバ１，２に振り分けて送信する。暗号プロトコル変換サーバ１，２は、各々分担して、端末１０Ａ－１から送信されたデータを、Ｃ１を使用して復号化した後、Ｃ２を使用して再暗号化する暗号変換処理を行ってから、端末１０Ｂ－１に送信する。端末１０Ｂ－１は、暗号プロトコル変換サーバ１，２から各々送信された２個のデータから、元の送信データを復元する。

図１



1

【特許請求の範囲】

【請求項１】第１の暗号を使用する１個以上の第１種の端末と、上記第１の暗号とは異なる第２の暗号を使用する１個以上の第２種の端末と、上記第１の暗号および上記第２の暗号を使用するｎ（ｎ≧２）個の暗号プロトコル変換サーバとが、１個以上のネットワークで接続された暗号通信システムであって、

上記第１種の端末は、各々、

上記第２種の端末のうちのいずれかの端末に送信すべきデータから、上記ｎ個の暗号プロトコル変換サーバのうちのｋ（ｎ≧ｋ≧２）個の暗号プロトコル変換サーバに振り分けるべきｋ個のデータを生成する振り分け手段と、上記振り分け手段が生成したｋ個のデータを、上記第１の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したｋ個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記ｋ個の暗号プロトコル変換サーバに送信する送信手段とを有し、

上記ｎ個の暗号プロトコル変換サーバは、各々、

上記第１種の端末のうちのいずれかの端末から送信された１個のデータを、上記第１の暗号で復号化した後、上記第２の暗号で再暗号化する暗号変換手段と、上記暗号変換手段が再暗号化した１個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段とを有し、

上記第２種の端末は、各々、

上記ｋ個の暗号プロトコル変換サーバの各々から送信されたｋ個のデータを、上記第２の暗号で復号化する復号化手段と、上記復号化手段が復号化したｋ個のデータから、元のデータを復元する復元手段とを有することを特徴とする暗号通信システム。

【請求項２】第１の暗号を使用する１個以上の第１種の端末と、上記第１の暗号とは異なる第２の暗号を使用する１個以上の第２種の端末と、上記第１の暗号および上記第２の暗号を使用するｎ（ｎ≧２）個の暗号プロトコル変換サーバとが、１個以上のネットワークで接続された暗号通信システムであって、

上記第１種の端末は、各々、

上記第２種の端末のうちのいずれかの端末に送信すべきデータから、上記ｎ個の暗号プロトコル変換サーバのうちのｋ（ｎ≧ｋ≧２）個の暗号プロトコル変換サーバに振り分けるべきｋ個のデータを生成する振り分け手段と、上記振り分け手段が生成したｋ個のデータを、上記第１の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したｋ個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記ｋ個の暗号プロトコル変換サーバに送信する送信手段と、上記ｋ個の暗号プロトコル変換サーバの各々から送信されたｋ個のデータを、上記第１の暗号で復号化する復号化手段と、上記復号化手段が復号化したｋ個のデータから、元のデータを復元する復元手段とを有し、

上記第２種の端末は、各々、

上記第１種の端末のうちのいずれかの端末に送信すべきデータから、上記ｎ個の暗号プロトコル変換サーバのうちのｋ（ｎ≧ｋ≧２）個の暗号プロトコル変換サーバに振り分けるべきｋ個のデータを生成する振り分け手段と、上記振り分け手段が生成したｋ個のデータを、上記第２の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したｋ個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記ｋ個の暗号プロトコル変換サーバに送信する送信手段と、上記ｋ個の暗号プロトコル変換サーバの各々から送信されたｋ個のデータを、上記第２の暗号で復号化する復号化手段と、上記復号化手段が復号化したｋ個のデータから、元のデータを復元する復元手段とを有し、

上記ｎ個の暗号プロトコル変換サーバは、各々、

上記第１種の端末および上記第２種の端末のうちのいずれかの端末から送信された１個のデータを、上記第１の暗号および上記第２の暗号のうちの、該データに付加されている端末情報が示す送信元の端末が使用する暗号で復号化した後、上記第１の暗号および上記第２の暗号のうちの、該データに付加されている端末情報が示す送信先の端末が使用する暗号で再暗号化する暗号変換手段と、上記暗号変換手段が再暗号化した１個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段とを有することを特徴とする暗号通信システム。

【請求項３】第１の暗号を使用する１個以上の第１種の端末と、上記第１の暗号とは異なる第２の暗号を使用する１個以上の第２種の端末と、上記第１の暗号、並びに、上記第１の暗号および上記第２の暗号とは異なる第３の暗号を使用するｎ個（ｎ≧２）の第１種の暗号プロトコル変換サーバと、上記第２の暗号および上記第３の暗号を使用し、上記ｎ個の第１種の暗号プロトコルサーバの各々に予め対応付けられたｎ（ｎ≧２）個の第２種の暗号プロトコル変換サーバとが、１個以上のネットワークで接続された暗号通信システムであって、

上記第１種の端末は、各々、

上記第２種の端末のうちのいずれかの端末に送信すべきデータから、上記ｎ個の第１種の暗号プロトコル変換サーバのうちのｋ（ｎ≧ｋ≧２）個の暗号プロトコル変換サーバに振り分けるべきｋ個のデータを生成する振り分け手段と、上記振り分け手段が生成したｋ個のデータを、上記第１の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したｋ個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記ｋ個の第１種の暗号プロトコル変換サーバに送信する送信手段と、上記ｋ個の第１種の暗号プロトコル変換サーバの各々から送信されたｋ個のデータを、上記第１の暗号で復号化する復号化手段と、上記復号化手段が復号

化したｋ個のデータから、元のデータを復元する復元手段とを有し、

上記第２種の端末は、各々、

上記第１種の端末のうちのいずれかの端末に送信すべきデータから、上記ｎ個の第２種の暗号プロトコル変換サーバのうちのｋ（ｎ≧ｋ≧２）個の暗号プロトコル変換サーバに振り分けるべきｋ個のデータを生成する振り分け手段と、上記振り分け手段が生成したｋ個のデータを、上記第２の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したｋ個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記ｋ個の第２種の暗号プロトコル変換サーバに送信する送信手段と、上記ｋ個の第２種の暗号プロトコル変換サーバの各々から送信されたｋ個のデータを、上記第２の暗号で復号化する復号化手段と、上記復号化手段が復号化したｋ個のデータから、元のデータを復元する復元手段とを有し、

上記ｎ個の第１種の暗号プロトコル変換サーバは、各々、

上記第１種の端末のうちのいずれかの端末から送信された１個のデータを、上記第１の暗号で復号化した後、上記第３の暗号で再暗号化し、また、上記ｎ個の第２種の暗号プロトコル変換サーバのうちの、対応する１個の暗号プロトコル変換サーバから送信された１個のデータを、上記第３の暗号で復号化した後、上記第１の暗号で再暗号化する暗号変換手段と、上記暗号変換手段が上記第３の暗号で再暗号化した１個のデータを、上記ｎ個の第２種の暗号プロトコル変換サーバのうちの、対応する１個の暗号プロトコル変換サーバに送信し、また、上記暗号変換手段が上記第１の暗号で再暗号化した１個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段とを有し、

上記ｎ個の第２種の暗号プロトコル変換サーバは、各々、

上記第２種の端末のうちのいずれかの端末から送信された１個のデータを、上記第２の暗号で復号化した後、上記第３の暗号で再暗号化し、また、上記ｎ個の第１種の暗号プロトコル変換サーバのうちの、対応する１個の暗号プロトコル変換サーバから送信された１個のデータを、上記第３の暗号で復号化した後、上記第２の暗号で再暗号化する暗号変換手段と、上記暗号変換手段が上記第３の暗号で再暗号化した１個のデータを、上記ｎ個の第１種の暗号プロトコル変換サーバのうちの、対応する１個の暗号プロトコル変換サーバに送信し、また、上記暗号変換手段が上記第２の暗号で再暗号化した１個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段とを有することを特徴とする暗号通信システム。

【請求項４】請求項１，２または３記載の暗号通信システムにおいて、

上記振り分け手段は、データ量が均等で、かつ、生成前のデータのデータ量よりデータ量が小さいｋ個のデータを生成することを特徴とする暗号通信システム。

【請求項５】請求項１，２または３記載の暗号通信システムにおいて、

上記振り分け手段は、排他的論理和を取ると生成前のデータと等しくなるようなｋ個のデータを生成することを特徴とする暗号通信システム。

【請求項６】請求項１，２，３または４記載の暗号通信システムにおいて、

上記振り分け手段は、生成前のデータが一定のデータ量ごとに順次割り当てられたｋ個のデータを生成することを特徴とする暗号通信システム。

【請求項７】請求項１～６のいずれか記載の暗号通信システムにおいて、

上記振り分け手段は、生成前のデータを一定のデータ量単位でスクランブルした後、スクランブル後のデータからｋ個のデータを生成することを特徴とする暗号通信システム。

【請求項８】請求項６または７記載の暗号通信システムにおいて、

上記生成前のデータが文字列を表す場合に、上記一定のデータ量は、１文字分のデータより小さいことを特徴とする暗号通信システム。

【請求項９】請求項１～８のいずれか記載の暗号通信システムにおいて、

上記暗号変換手段は、一定のデータ量ごとに、復号化および再暗号化を行うことを特徴とする暗号通信システム。

【請求項１０】第１の暗号を使用する１個以上の第１種の端末と、上記第１の暗号とは異なる第２の暗号を使用する１個以上の第２種の端末と、上記第１の暗号および上記第２の暗号を使用し、一方の暗号で暗号化されたデータをもう一方の暗号で暗号化されたデータに暗号変換するｎ（ｎ≧２）個の暗号プロトコル変換サーバとが、１個以上のネットワークで接続された暗号通信システムにおいて、上記第１種の端末として用いられる情報処理装置であって、

上記第２種の端末のうちのいずれかの端末に送信すべきデータから、上記ｎ個の暗号プロトコル変換サーバのうちのｋ（ｎ≧ｋ≧２）個の暗号プロトコル変換サーバに振り分けるべきｋ個のデータを生成する振り分け手段と、上記振り分け手段が生成したｋ個のデータを、上記第１の暗号で暗号化する暗号化手段と、上記暗号化手段が暗号化したｋ個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記ｋ個の暗号プロトコル変換サーバに送信する送信手段と、上記ｋ個の暗号プロトコル変換サーバの各々から送信されたｋ個のデータを、上記第１の暗号で復号化する復号化手段と、上記復号化手段が復号化したｋ個のデータから、

元のデータを復元する復元手段とを有することを特徴とする情報処理装置。

【請求項１１】請求項１０記載の情報処理装置において、

上記振り分け手段は、排他的論理和を取ると生成前のデータと等しくなるようなｋ個のデータを生成することを特徴とする情報処理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、互いに異なる暗号を使用する端末間で暗号通信を行うことを可能とする暗号通信システムに関するものである。

【０００２】

【従来の技術】従来、使用されてきた暗号には、アルゴリズム秘匿型とアルゴリズム公開型があり、前者は、軍隊等で隠密に使用され、後者は、アルゴリズムを一般に公開した上で、銀行等で使用されている。いずれの場合も、１種類の暗号を使用し、閉じたネットワーク内で暗号通信が行われている。

【０００３】近年のコンピュータ利用形態のオープン化，マルチベンダ化，インターネット化に伴い、互いに異なるアルゴリズム公開型の暗号を使用する端末が接続されたネットワークを相互接続し、これらのネットワークに各々接続された端末間でも暗号通信を行いたいという要求が生じることが予想される。

【０００４】一方、国際標準化機構ＩＳＯ（International Organization for Standardization）は、１９９１年に、暗号アルゴリズム登録制度を設立し、暗号アルゴリズムについては１種類に標準化せず、認可登録された複数種類の暗号アルゴリズムを一般に提供していくことを決定した。その結果，将来においても、複数種類の暗号アルゴリズムが地域ごとに使い分けられていく可能性が生じた。日本においても、１９９４年ＩＳＯの暗号アルゴリズム登録制度のＪＩＳ（Japanese Industrial Standards）化を行っている。

【０００５】互いに異なる暗号を使用する端末が接続されたネットワークを相互接続した場合、これらのネットワークに各々接続された端末間で暗号通信を行うためには、送信元の端末が、送信すべきデータを自身が使用する暗号で暗号化することしかできず、送信先の端末が、自身が使用する暗号で暗号化されたデータしか復号化することができないことから、一旦、送信元の端末が暗号化した送信データを、送信先の端末が使用する暗号で暗号化したデータに変換する必要が生じる。

【０００６】このような暗号変換処理に関する公知技術としては、財団法人日本規格協会の調査研究報告書「平成３年度多目的利用ＩＣカード社会における望ましいシステム構築とあるべき標準化に関する調査研究報告書」（日機連３標準化－２０，平成４年３月，２５頁～３１頁）において、暗号プロトコル変換装置が開示されている。

【０００７】この暗号プロトコル変換装置は、互いに異なる暗号を使用する端末が接続された２個のネットワークを結ぶ通信回線上に設置され、これら２個のネットワークで各々使用されている２種類の暗号アルゴリズム（暗号化アルゴリズムおよび復号化アルゴリズム）を備えるようにしている。

【０００８】そして、暗号プロトコル変換装置は、送信元の端末が使用する暗号で暗号化されている送信データを、装置内に備えている、送信元の端末が使用する暗号の復号化アルゴリズムで復号化し、さらに、復号化したデータを、装置内に備えている、送信先の端末が使用する暗号の暗号化アルゴリズムで暗号化するという暗号変換処理を行う。

【０００９】

【発明が解決しようとする課題】しかしながら、上述した暗号プロトコル変換装置においては、送信元の端末が暗号化したデータが、一旦、復号化されることから、暗号化される前のデータである「平文」の状態となり、第三者が平文を盗むチャンスが存在してしまい、データの秘匿性が破られる危険性がある。

【００１０】そこで、本発明の第１の目的は、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、安全に行うことが可能な暗号通信システムを提供することにある。

【００１１】また、上述した公知技術を開示する調査研究報告書においては、暗号プロトコル変換装置が１個のみ設置されている。送信すべきデータのデータ量が多い場合は、暗号プロトコル変換装置が１個のみでは、暗号変換処理を高速に行うことはできず、暗号変換処理に関するオーバヘッドが大きくなると考えられる。

【００１２】将来的には、テラ（１テラ＝１ギガ×１０００）ｂｐｓに及ぶ大容量通信の時代が到来することが予想されており、このような大容量通信の時代には、通信路の高速化が重要な課題である。

【００１３】そこで、本発明の第２の目的は、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、高速に行うことが可能な暗号通信システムを提供することにある。

【００１４】さらに、上述した暗号プロトコル変換装置は、各端末が使用する２種類の暗号アルゴリズム（暗号化アルゴリズムおよび復号化アルゴリズム）を備えるようにしているが、これらの端末が各々接続されたネットワークが異なる国に属する場合には、必ずしも実現可能ではない。実際、例えば、米国は、法律により、暗号技術（米国暗号標準ＤＥＳ等）の輸出入を規制している。このような規制が適用された場合、自国に属するネットワークに接続された端末が使用する暗号アルゴリズムを他国内に設置された暗号プロトコル変換装置に備えることができず、暗号通信を行うことができなくなる。

【００１５】そこで、本発明の第３の目的は、互いに異なる暗号を使用する端末が異なる国に属する場合でも、上記第１の目的を達成することが可能な暗号通信システムを提供することにある。

【００１６】

【課題を解決するための手段】上記第１の目的を達成するために、本発明においては、互いに異なる暗号を使用する端末間で送受信するデータが、複数の暗号プロトコル変換サーバを経由するようにし、これらの複数の暗号プロトコル変換サーバが分担して上述した暗号変換処理を行うようにしている。そして、複数の暗号プロトコル変換サーバに暗号変換処理を分担させるために、送信元の端末が、送信すべきデータから、複数の暗号プロトコル変換サーバに振り分けるべき複数のデータを生成するようにしている。

【００１７】そのために、本発明は、第１の暗号を使用する１個以上の第１種の端末と、上記第１の暗号とは異なる第２の暗号を使用する１個以上の第２種の端末と、上記第１の暗号および上記第２の暗号を使用するｎ（ｎ≧２）個の暗号プロトコル変換サーバとが、１個以上のネットワークで接続された暗号通信システムを提供しており、上記第１種の端末が、各々、（１）上記第２種の端末のうちのいずれかの端末に送信すべきデータから、上記ｎ個の暗号プロトコル変換サーバのうちのｋ（ｎ≧ｋ≧２）個の暗号プロトコル変換サーバに振り分けるべきｋ個のデータを生成する振り分け手段、（２）上記振り分け手段が生成したｋ個のデータを、上記第１の暗号で暗号化する暗号化手段、（３）上記暗号化手段が暗号化したｋ個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記ｋ個の暗号プロトコル変換サーバに送信する送信手段、（４）上記ｋ個の暗号プロトコル変換サーバの各々から送信されたｋ個のデータを、上記第１の暗号で復号化する復号化手段、（５）上記復号化手段が復号化したｋ個のデータから、元のデータを復元する復元手段、を有するようにし、上記第２種の端末が、各々、（１）上記第１種の端末のうちのいずれかの端末に送信すべきデータから、上記ｎ個の暗号プロトコル変換サーバのうちのｋ（ｎ≧ｋ≧２）個の暗号プロトコル変換サーバに振り分けるべきｋ個のデータを生成する振り分け手段、（２）上記振り分け手段が生成したｋ個のデータを、上記第２の暗号で暗号化する暗号化手段、（３）上記暗号化手段が暗号化したｋ個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記ｋ個の暗号プロトコル変換サーバに送信する送信手段、（４）上記ｋ個の暗号プロトコル変換サーバの各々から送信されたｋ個のデータを、上記第２の暗号で復号化する復号化手段、（５）上記復号化手段が復号化したｋ個のデータから、元のデータを復元する復元手段、を有するようにし、上記ｎ個の暗号プロトコル変換サーバが、各々、（１）上記第１種の端末および上記第２種の端末のうちのいずれかの端末から送信された１個のデータを、上記第１の暗号および上記第２の暗号のうちの、該データに付加されている端末情報が示す送信元の端末が使用する暗号で復号化した後、上記第１の暗号および上記第２の暗号のうちの、該データに付加されている端末情報が示す送信先の端末が使用する暗号で再暗号化する暗号変換手段、（２）上記暗号変換手段が再暗号化した１個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段、を有するようにしている。

【００１８】例えば、上記振り分け手段は、排他的論理和を取ると生成前のデータと等しくなるようなｋ個のデータを生成するようにすることができる。このとき、さらに、上記振り分け手段は、生成前のデータを一定のデータ量単位でスクランブルした後、スクランブル後のデータからｋ個のデータを生成するようにしてもよい。なお、一定のデータ量が、１文字分のデータより小さいデータ量であることが好ましい。

【００１９】また、例えば、上記暗号変換手段は、一定のデータ量ごとに、復号化および再暗号化を行うようにすることができる。

【００２０】また、上記第２の目的を達成するために、本発明においては、複数の暗号プロトコル変換サーバが分担して暗号変換処理を行うデータ、すなわち、送信元の端末が生成する複数のデータの各々が、元のデータのデータ量よりデータ量が小さいデータであるようにしている。

【００２１】すなわち、上記振り分け手段は、データ量が均等で、かつ、生成前のデータのデータ量より小さいｋ個のデータを生成するようにしている。

【００２２】例えば、上記振り分け手段は、生成前のデータが一定のデータ量ごとに順次割り当てられたｋ個のデータを生成するようにすることができる。このとき、さらに、上記振り分け手段は、生成前のデータを一定のデータ量単位でスクランブルした後、スクランブル後のデータからｋ個のデータを生成するようにしてもよい。

【００２３】また、上記第３の目的を達成するために、本発明においては、互いに異なる暗号を使用する端末が異なる国に属する場合に、これらの国が共通に使用するよう協定した１個の暗号を利用し、これらの端末間で送受信されるデータが、国境を越えるときには、該協定した暗号で暗号化された状態となるようにしている。

【００２４】このように、協定した暗号を利用することで、各暗号プロトコル変換サーバは、自身が属する国とは異なる国に属する端末が使用する暗号を使用する必要がなくなり、上記第１の目的を達成するための暗号通信システムを構築することができるようになる。

【００２５】そのために、本発明は、第１の暗号を使用する１個以上の第１種の端末と、上記第１の暗号とは異なる第２の暗号を使用する１個以上の第２種の端末と、

上記第1の暗号、並びに、上記第1の暗号および上記第2の暗号とは異なる第3の暗号を使用するn個（n≧2）の第1種の暗号プロトコル変換サーバと、上記第2の暗号および上記第3の暗号を使用し、上記n個の第1種の暗号プロトコルサーバの各々に予め対応付けられたn（n≧2）個の第2種の暗号プロトコル変換サーバとが、1個以上のネットワークで接続された暗号通信システムを提供しており、上記第1種の端末が、各々、

（1）上記第2種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の第1種の暗号プロトコル変換サーバのうちのk（n≧k≧2）個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段、（2）上記振り分け手段が生成したk個のデータを、上記第1の暗号で暗号化する暗号化手段、（3）上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の第1種の暗号プロトコル変換サーバに送信する送信手段、（4）上記k個の第1種の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第1の暗号で復号化する復号化手段、（5）上記復号化手段が復号化したk個のデータから、元のデータを復元する復元手段、を有するようにし、上記第2種の端末が、各々、（1）上記第1種の端末のうちのいずれかの端末に送信すべきデータから、上記n個の第2種の暗号プロトコル変換サーバのうちのk（n≧k≧2）個の暗号プロトコル変換サーバに振り分けるべきk個のデータを生成する振り分け手段、（2）上記振り分け手段が生成したk個のデータを、上記第2の暗号で暗号化する暗号化手段、（3）上記暗号化手段が暗号化したk個のデータを、各々、送信元の端末および送信先の端末を示す端末情報を付加して、上記k個の第2種の暗号プロトコル変換サーバに送信する送信手段、（4）上記k個の第2種の暗号プロトコル変換サーバの各々から送信されたk個のデータを、上記第2の暗号で復号化する復号化手段、（5）上記復号化手段が復号化したk個のデータから、元のデータを復元する復元手段、を有するようにし、上記n個の第1種の暗号プロトコル変換サーバが、各々、（1）上記第1種の端末のうちのいずれかの端末から送信された1個のデータを、上記第1の暗号で復号化した後、上記第3の暗号で再暗号化し、また、上記n個の第2種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバから送信された1個のデータを、上記第3の暗号で復号化した後、上記第1の暗号で再暗号化する暗号変換手段、

（2）上記暗号変換手段が上記第3の暗号で再暗号化した1個のデータを、上記n個の第2種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバに送信し、また、上記暗号変換手段が上記第1の暗号で再暗号化した1個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段、を有するようにし、上記n個の第2種の暗号プロトコル変換サーバが、各々、（1）上記第2種の端末のうちのいずれかの端末から送信された1個のデータを、上記第2の暗号で復号化した後、上記第3の暗号で再暗号化し、また、上記n個の第1種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバから送信された1個のデータを、上記第3の暗号で復号化した後、上記第2の暗号で再暗号化する暗号変換手段、（2）上記暗号変換手段が上記第3の暗号で再暗号化した1個のデータを、上記n個の第1種の暗号プロトコル変換サーバのうちの、対応する1個の暗号プロトコル変換サーバに送信し、また、上記暗号変換手段が上記第2の暗号で再暗号化した1個のデータを、該データに付加されている端末情報が示す送信先の端末に送信する送信手段、を有するようにしている。

【0026】

【作用】本発明の暗号通信システムによれば、送信元の端末において、上記振り分け手段が、送信すべきデータから、平文状態で意味判別困難な複数のデータを生成するようにしていると共に、複数の暗号プロトコル変換サーバが暗号変換処理を分担して行うようにしているので、全ての暗号プロトコル変換サーバから平文状態のデータが盗まれたとしても、複数のデータの生成方法が知られない限り、データの秘匿性は守られることとなり、逆に、複数のデータの生成方法が知られたとしても、全ての暗号プロトコル変換サーバから平文状態のデータが盗まれない化ぎり、データの秘匿性は守られることとなる。

【0027】また、例えば、暗号プロトコル変換サーバにおいて、上記暗号変換手段が、一定のデータ量ごとに暗号変換処理を行うようにすれば、同時に平文状態となるデータの量が、該一定のデータ量のみとなるので、データが平文状態となる時間が短くなり、また、この時間に平文状態のデータが盗まれても、該一定のデータ量のデータのみが判別するだけで済む。

【0028】さらに、送信元の端末において、上記振り分け手段が、送信すべきデータから、該データのデータ量よりデータ量が小さい複数のデータを生成するようにすれば、複数の暗号プロトコル変換サーバ間で負荷が分散され、各暗号プロトコル変換サーバが行う暗号変換処理の負荷が軽減される。

【0029】

【実施例】以下、本発明の実施例について図面を参照して説明する。

【0030】図1は本発明の第1の実施例の暗号通信システムの構成図である。

【0031】図1に示した暗号通信システムは、互いに異なる暗号を使用する2個のLAN（Local Area Network）であるLAN－A（100A），LAN－B（100B）に各々接続されている任意の端末間で、暗号通信

を行うためのものである。

【００３２】この暗号通信は、ＷＡＮ（Wide Area Network）１１０，暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）を経由して行われる。

【００３３】図１に示すように、ＬＡＮ－Ａ（１００Ａ）は、暗号アルゴリズムＣ１（１２）を備え、これを使用する複数の端末１０Ａ－１～１０Ａ－ｍが接続されたローカルエリア・ネットワークであり、ＬＡＮ－Ｂ（１００Ｂ）は、暗号アルゴリズムＣ２（１３）を備え、これを使用する複数の端末１０Ｂ－１～１０Ｂ－ｎが接続されたローカルエリア・ネットワークであり、各々、通信回線２０，２１を介して、ＷＡＮ１１０と接続されている。

【００３４】また、暗号プロトコル変換サーバ１（３０Ａ）が属する第三機関ＡのＬＡＮ（１２０Ａ）、および、暗号プロトコル変換サーバ２（３０Ｂ）が属する第三機関ＢのＬＡＮ（１２０Ｂ）が、各々、通信回線２２，２３を介して、ＷＡＮ１１０と接続されている。

【００３５】以下、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１からＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１に対する暗号通信を例にして、暗号通信システムの動作概要を説明する。

【００３６】送信元の端末１０Ａ－１は、送信先の端末１０Ｂ－１に送信すべきデータを、自身が備えている振り分けプログラム１１を使用して２個に振り分ける振り分け処理を行う。そして、端末１０Ａ－１は、振り分け処理を行った後の一方のデータを、自身が備えているアルゴリズムＣ１（１２）を使用して暗号化し、ＷＡＮ１１０を経由して、暗号プロトコル変換サーバ１（３０Ａ）に送信する。また、もう一方のデータを、自身が備えているアルゴリズムＣ１（１２）を使用して暗号化し、ＷＡＮ１１０を経由して、暗号プロトコル変換サーバ２（３０Ｂ）に送信する。

【００３７】暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）は、各々、端末１０Ａ－１から送信されたデータを、自身が備えているアルゴリズムＣ１（３１Ａ，３１Ｂ）を使用して復号化し、さらに、受信先の端末１０Ｂ－１が備えているアルゴリズムＣ２（１３）と同じアルゴリズムＣ２（３２Ａ，３２Ｂ）を使用して再暗号化するという暗号変換処理を行う。そして、暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）は、各々、暗号変換処理を行った後のデータを、ＷＡＮ１１０を介して受信先の端末１０Ｂ－１に送信する。

【００３８】受信先の端末１０Ｂ－１は、暗号プロトコル変換サーバ１（３０Ａ）から送信されたデータ、および、暗号プロトコル変換サーバ２（３０Ｂ）から送信されたデータを、各々、自身が備えているアルゴリズムＣ２（１３）を使用して復号化し、さらに、復号化した２個のデータを、自身が備えている復元プログラム１４を使用して、元のデータに復元する。

【００３９】本実施例は、振り分けプログラム１１による振り分け方法を工夫することで、従来は暗号変換処理時に平文状態となっていたデータの秘匿性を高めることを特徴とするものである。以下、振り分け方法の具体例を含め、暗号通信システムに関するさらに詳細な説明を行う。

【００４０】なお、以下の説明においては、ＬＡＮ－Ａ（１００Ａ）とＬＡＮ－Ｂ（１００Ｂ）とが、互いに異なる同ブロック長のブロック型慣用暗号を使用している場合に、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１からＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１に対する暗号通信を例にして、暗号通信システムの詳細な動作について説明する。

【００４１】まず、送信元の端末１０Ａ－１の動作について説明する。

【００４２】図２は端末１０Ａ－１のハードウェアの主要部分を示す構成図である。

【００４３】図２に示すように、端末１０Ａ－１は、演算処理を行うＣＰＵ（Central Processing Unit）２０１と、データを記憶するための主記憶装置２０２および２次記憶装置２０３と、端末外部との間の通信を制御する通信アダプタ２０４と、これらを接続するバス２０５とから構成されており、通信アダプタ２０４を介して、通信回線２０６により、ＬＡＮ－Ａ（１００Ａ）と接続されている。

【００４４】図３は端末１０Ａ－１の主記憶装置２０２の利用形態を示す説明図である。

【００４５】図３に示すように、主記憶装置２０２上には、ＬＡＮ－Ａ（１００Ａ）で使用されている暗号アルゴリズムＣ１を用いたＣ１暗号化プログラム３０１およびＣ１復号化プログラム３０２と、送信すべきデータを振り分けるための振り分けプログラム３０３と、暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）から送信されたデータを、元のデータに復元するための復元プログラム３０４とが格納され、また、ワークエリア３０５が確保されている。

【００４６】さらに、暗号通信の送受信時に使用する情報として、暗号プロトコル変換サーバ１（３０Ａ）との間の暗号通信用の鍵ＫＡＡ１（３０６）および暗号用初期値（乱数）Ａ１（３０７）と、暗号プロトコル変換サーバ２（３０Ｂ）との間の暗号通信用の鍵ＫＢＡ１（３０８）および暗号用初期値（乱数）Ａ２（３０９）と、端末１０Ａ－１自身の端末識別子３１０と、暗号プロトコル変換サーバ１（３０Ａ）のサーバ識別子３１１と、暗号プロトコル変換サーバ２（３０Ｂ）のサーバ識別子３１２とが格納されている。

【００４７】図４は端末１０Ａ－１の送信処理手順を示すフローチャートである。

【００４８】図４に示すように、端末１０Ａ－１は、暗号通信の送信要求が入力されると、まず、該送信要求と共に送信者が入力した送信先の端末の端末識別子（ここでは、端末１０Ｂ－１の端末識別子）を、ワークエリア３０５に設定する（ステップ４０１）。

【００４９】続いて、ステップ４０１でワークエリア３０５に設定した端末の端末識別子（ここでは、端末１０Ｂ－１の端末識別子）に基づいて、送信先の端末が接続されたＬＡＮ（ここでは、ＬＡＮ－Ｂ（１００Ｂ））を判断する（ステップ４０２）。

【００５０】続いて、Ｃ１暗号化プログラム３０１のパラメータとなる、暗号プロトコル変換サーバ１（３０Ａ）との間の暗号通信用の鍵ＫＡＡ１（３０６）および暗号用初期値Ａ１（３０７）をワークエリア３０５に設定する（ステップ４０３）。ここで、暗号用初期値Ａ１（３０７）は、ＣＢＣ（Cipher Block Chainning：暗号文ブロック連鎖）モードでの暗号化／復号化に使用する定数（乱数）である。なお、ＣＢＣモードについては後述する。

【００５１】続いて、Ｃ１暗号化プログラム３０１のパラメータとなる、暗号プロトコル変換サーバ２（３０Ｂ）との間の暗号通信用の鍵ＫＢＡ１（３０８）および暗号用初期値Ａ２（３０９）をワークエリア２０５に設定する（ステップ４０４）。暗号用初期値Ａ２（３０９）の役割は、暗号用初期値Ａ１（３０７）の役割と同様である。

【００５２】続いて、予め作成されて２次記憶装置２０３上のファイルＡに格納されている平文状態のデータであって、端末１０Ｂ－１に送信すべきデータを、ワークエリア３０５にロードする（ステップ４０５）。

【００５３】続いて、振り分けプログラム３０３を用いて、ステップ４０５でワークエリア３０５にロードしたデータを、２個の暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）に各々振り分けるための振り分け処理を行う（ステップ４０６）。

【００５４】ここで、振り分けプログラム１１による振り分け方法の具体例について、図５を用いて説明する。

【００５５】図５に示す例では、元のデータｄと任意の乱数ａｌとに基づいて、排他的論理和を利用して、２個の暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）に各々振り分けるデータａ，ｂを生成している。

【００５６】詳しくは、まず、任意の乱数をａｌに与え、ｄｌとａｌとの間で排他的論理和を取った結果を、ｂｌとする。続いて、ｂｌをａ２とし、ｄ２とａ２との間で排他的論理和を取った結果を、ｂ２とする。同様な処理を行うと、ｄｌ～ｄｌ０からなる元のデータｄから、ａｌ～ａｌ０からなるデータａと、ｂｌ～ｂｌ０からなるデータｂとが生成される。

【００５７】このようにして生成されたデータａ，ｂは、各々、その内容が撹乱されており、それ自体としては意味判別困難である。

【００５８】なお、振り分け方法としては、この例に限らず、２個の暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）のいずれか一方において、平文状態のデータが盗まれた場合でも、該一方のデータだけでは意味判別困難であるような振り分け方法であればよい。

【００５９】さて、図４に戻って、端末１０Ａ－１は、ステップ４０３で設定したパラメータをＣ１暗号化プログラム３０１に与えて、Ｃ１暗号化プログラム３０１を実行し、暗号プロトコル変換サーバ１（３０Ａ）に振り分けるデータ（ここでは、データａ）をＣＢＣモードで暗号化する（ステップ４０７）。

【００６０】ここで、ＣＢＣモードでの暗号化について、図６を用いて説明する。

【００６１】図６に示すように、ＣＢＣモードは、暗号強度を増加させるために、現在通常使用（ＩＳＯで標準化済み）されている暗号利用モードであり、暗号化された１データブロックを、次に暗号化する１データブロックに排他的論理和を取ることで絡ませて、次々と連鎖させて暗号化している手法である。ブロック型慣用暗号の利用モードについては、「現代暗号理論」（電子通信学会）の６４頁～７６頁に記載されている。

【００６２】再び、図４に戻って、端末１０Ａ－１は、ステップ４０４で設定したパラメータをＣ１暗号化プログラム３０１に与えて、Ｃ１暗号化プログラム３０１を実行し、暗号プロトコル変換サーバ２（３０Ｂ）に振り分けるデータ（ここでは、データｂ）をＣＢＣモードで暗号化する（ステップ４０８）。

【００６３】続いて、暗号プロトコル変換サーバ１（３０Ａ）経由の暗号通信で使用するヘッダ情報を作成するための領域、および、暗号プロトコル変換サーバ２（３０Ｂ）経由の暗号通信で使用するヘッダ情報を作成するための領域を、ワークエリア３０５に確保する（ステップ４０９）。

【００６４】続いて、ステップ４０９で確保した領域に、図７に示す形式７００に基づいて、ヘッダ情報を設定する（ステップ４１０）。具体的には、ステップ４０１でワークエリア３０５に設定した端末１０Ｂ－１の端末識別子，送信元の端末である端末１０Ａ－１自身の端末識別子３１０，暗号プロトコル変換サーバ１（３０Ａ）のサーバ識別子３１１からなるヘッダ情報７０１（図７においては、各々，７０１０，７０１１，７０１２としている。）を、一方の領域に設定し、ステップ４０１でワークエリア３０５に設定した端末１０Ｂ－１の端末識別子，送信元の端末である端末１０Ａ－１自身の端末識別子３１０，暗号プロトコル変換サーバ２（３０Ｂ）のサーバ識別子３１２からなるヘッダ情報７０２

（図７においては、各々、７０２０，７０２１，７０２２としている。）を、もう一方の領域に設定する。

【００６５】続いて、ステップ４１０で設定したヘッダ情報７０１を先頭に添付しながら、ステップ４０７で暗号化したデータを、ファイルＡ１に格納し、また、ステップ４１０で設定したヘッダ情報７０２を先頭に添付しながら、ステップ４０８で暗号化したデータを、ファイルＡ２に格納する（ステップ４１１）。

【００６６】続いて、ファイルＡ内に未暗号化データが格納されているか否かを判定し（ステップ４１２）、格納されているならば、ステップ４０５～ステップ４１１を繰り返す。ただし、ヘッダ情報７０１，７０２は、ファイルＡ１，Ａ２の先頭にのみ添付するものとする。実際には、送信単位であるバケット単位でヘッダ情報が必要となるが、ここでは、説明を簡単にするために、送信単位がファイル単位であるものとする。

【００６７】また、ファイルＡ内に未暗号化データが格納されていなければ、ファイルＡ１，Ａ２を、各々、ＷＡＮ１１０を介して、暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）に送信する（ステップ４１３）。

【００６８】次に、暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）の動作について説明する。

【００６９】図８は暗号プロトコル変換サーバ１（３０Ａ）のハードウェアの主要部分を示す構成図である。

【００７０】図８に示すように、暗号プロトコル変換サーバ１（３０Ａ）は、演算処理を行うＣＰＵ８０１と、データを記憶するための主記憶装置８０２および２次記憶装置８０３と、暗号プロトコル変換サーバ外部との間の通信を制御する通信アダプタ８０４と、これらを接続するバス８０５とから構成されており、通信アダプタ８０４を介して、通信回線８０６により、第三機関ＡのＬＡＮ（１２０Ａ）と接続されている。

【００７１】なお、暗号プロトコル変換サーバ２（３０Ｂ）のハードウェアの主要部分を示す構成図も、図８と同様である。

【００７２】図９は暗号プロトコル変換サーバ１（３０Ａ）の主記憶装置８０２の利用形態を示す説明図である。

【００７３】図９に示すように、主記憶装置８０２上には、ＬＡＮ－Ａ（１００Ａ）で使用されている暗号アルゴリズムＣ１を用いたＣ１暗号化プログラム９０１およびＣ１復号化プログラム９０２と、ＬＡＮ－Ｂ（１００Ｂ）で使用されている暗号アルゴリズムＣ２を用いたＣ２暗号化プログラム９０３およびＣ２復号化プログラム９０４とが格納され、また、ワークエリア９０５が確保されている。

【００７４】さらに、暗号通信の送受信時に使用する情報として、端末１０Ａ－１～１０Ａ－ｍの各々との間の

暗号通信用の鍵が設定されている鍵エリアＡ（９０６）と、端末１０Ｂ－１～１０Ｂ－ｎの各々との間の暗号通信用の鍵が設定されている鍵エリアＢ（９０７）と、暗号用初期値Ａ１（９０８）および暗号用初期値Ｂ１（９０９）とが格納されている。

【００７５】実際には、鍵エリアＡ（９０６）には、端末１０Ａ－１～１０Ａ－ｍの端末識別子９０６１ごとに、対応する鍵９０６２が設定されている。また、鍵エリアＢ（９０７）には、端末１０Ｂ－１～１０Ｂ－ｎの端末識別子９０７１ごとに、対応する鍵９０７２が設定されている。ただし、安全性を考慮し、２個の鍵エリア９０６，９０７に設定されている鍵は、全て、互いに異なるようにする。

【００７６】また、暗号用初期値Ａ１（９０８）は、端末１０Ａ－１の主記憶装置２０２上に格納されている暗号用初期値Ａ１（３０７）と同じ値であり、暗号用初期値Ｂ１（９０９）は、図１２を用いて後述するが、端末１０Ｂ－１の主記憶装置１１０２上に格納されている暗号用初期値Ｂ１（１２０７）と同じ値である。

【００７７】なお、暗号プロトコル変換サーバ２（３０Ｂ）の主記憶装置８０２の利用形態を示す説明図も、図９と同様である。ただし、安全性を考慮し、暗号プロトコル変換サーバ２（３０Ｂ）の主記憶装置８０２上に格納されている鍵は、全て、暗号プロトコル変換サーバ１（３０Ａ）の主記憶装置８０２上に格納されている鍵とは異なるようにする。

【００７８】図１０は暗号プロトコル変換サーバ１（３０Ａ）の暗号変換処理手順を示すフローチャートである。

【００７９】なお、暗号プロトコル変換サーバ１（３０Ａ）において、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１～１０Ａ－ｍのうちのいずれかの端末（ここでは、１０Ａ－１）から送信されたデータ（ここでは、ファイルＡ１）は、２次記憶装置８０３上に格納される。

【００８０】図１０に示すように、暗号プロトコル変換サーバ１（３０Ａ）は、まず、２次記憶装置８０３上に格納されているファイルＡ１内のヘッダ情報７０１から、送信先の端末である端末１０Ｂ－１の端末識別子７０１０、および、送信元の端末である端末１０Ａ－１の端末識別子７０１１を読み出して、ワークエリア９０５に設定する（ステップ１００１）。

【００８１】続いて、ステップ１００１で読み出した送信元の端末１０Ａ－１の端末識別子７０１１と鍵エリアＡ（９０６）に設定されている端末識別子９０６１とのマッチングを行うことにより、送信元の端末１０Ａ－１と暗号プロトコル変換サーバ１（３０Ａ）との間の暗号通信用の鍵ＫＡＡ１を検索し、ワークエリア９０５に設定する（ステップ１００２）。

【００８２】続いて、ステップ１００１で読み出した送

信先の端末１０Ｂ－１の端末識別子７０１０と鍵エリアＢ（９０７）に設定されている端末識別子９０７１とのマッチングを行うことにより、送信元の端末１０Ｂ－１と暗号プロトコル変換サーバ１（３０Ａ）との間の暗号通信用の鍵ＫＡＢ１を検索し、ワークエリア９０５に設定する（ステップ１００３）。

【００８３】続いて、Ｃ１復号化プログラム９０２のパラメータとなる、ステップ１００２で読み出した鍵ＫＡＡ１および暗号用初期値Ａ１（９０８）をワークエリア９０５に設定する（ステップ１００４）。

【００８４】続いて、Ｃ２暗号化プログラム９０３のパラメータとなる、ステップ１００３で読み出した鍵ＫＡＢ１および暗号用初期値Ｂ１（９０９）をワークエリア９０５に設定する（ステップ１００５）。

【００８５】続いて、ファイルＡ１内のデータを、ワークエリア９０５にロードする（ステップ１００６）。

【００８６】続いて、ステップ１００６でロードしたファイルＡ１内のデータについて暗号変換処理を行う（ステップ１００７）。

【００８７】すなわち、まず、ステップ１００６でロードしたデータを、先頭から１ブロックずつ、ステップ１００４で設定したパラメータをＣ１復号化プログラム９０２に与えて、Ｃ１復号化プログラム９０２を実行して復号化し、さらに、ステップ１００５で設定したパラメータをＣ２暗号化プログラム９０３に与えて、Ｃ２暗号化プログラム９０３を実行して再暗号化する。なお、再暗号化されたデータは、ワークエリア９０５上の元の位置に格納される。

【００８８】ステップ１００７の暗号変換処理を終了すると、ワークエリア９０５上に格納されているデータ（再暗号化されたデータ）を、ファイルＢ１に格納する（ステップ１００８）。

【００８９】続いて、ファイルＡ１内に未変換データが格納されているか否かを判定し（ステップ１００９）、格納されているならば、ステップ１００６～ステップ１００８を繰り返す。

【００９０】また、ファイルＡ１内に未変換データが格納されていなければ、ファイルＢ１を、ＷＡＮ１１０を介して、ＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１に送信する（ステップ１０１０）。

【００９１】なお、暗号プロトコル変換サーバ２（３０Ｂ）の暗号変換処理手順を示すフローチャートも、図１０と同様である。すなわち、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１から送信されたファイルＡ２を、ファイルＢ２に変換し、ＷＡＮ１１０を介して、ＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１に送信する。

【００９２】次に、送信先の端末１０Ｂ－１の動作について説明する。

【００９３】図１１は端末１０Ｂ－１のハードウェアの主要部分を示す構成図である。

【００９４】図１１に示すように、端末１０Ｂ－１は、端末１０Ａ－１と同様に、演算処理を行うＣＰＵ１１０１と、データを記憶するための主記憶装置１１０２および２次記憶装置１１０３と、端末外部との間の通信を制御する通信アダプタ１１０４と、これらを接続するバス１１０５とから構成されており、通信アダプタ１１０４を介して、通信回線１１０６により、ＬＡＮ－Ｂ（１００Ｂ）と接続されている。

【００９５】図１２は端末１０Ｂ－１の主記憶装置１１０２の利用形態を示す説明図である。

【００９６】図１２に示すように、主記憶装置１１０２上には、ＬＡＮ－Ｂ（１００Ｂ）で使用されている暗号アルゴリズムＣ２を用いたＣ２暗号化プログラム１２０１およびＣ２復号化プログラム１２０２と、送信すべきデータを振り分けるための振り分けプログラム１２０３と、暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）から送信されたデータを、元のデータに復元するための復元プログラム１２０４とが格納され、また、ワークエリア１２０５が確保されている。

【００９７】さらに、暗号通信の送受信時に使用する情報として、暗号プロトコル変換サーバ１（３０Ａ）との間の暗号通信用の鍵ＫＡＢ１（１２０６）および暗号用初期値（乱数）Ｂ１（１２０７）と、暗号プロトコル変換サーバ２（３０Ｂ）との間の暗号通信用の鍵ＫＢＢ１（１２０８）および暗号用初期値（乱数）Ｂ２（１２０９）と、端末１０Ｂ－１自身の端末識別子１２１０と、暗号プロトコル変換サーバ１（３０Ａ）のサーバ識別子１２１１と、暗号プロトコル変換サーバ２（３０Ｂ）のサーバ識別子１２１２とが格納されている。

【００９８】図１３は端末１０Ｂ－１の受信処理手順を示すフローチャートである。

【００９９】なお、端末１０Ｂ－１において、暗号プロトコル変換サーバ１（３０Ａ）から送信されたファイル（ここでは、ファイルＢ１），および、暗号プロトコル変換サーバ２（３０Ｂ）から送信されたファイル（ここでは、ファイルＢ２）は、２次記憶装置１１０３上に格納される。

【０１００】図１３に示すように、端末１０Ｂ－１は、ファイルＢ１，Ｂ２の受信を完了すると、まず、２次記憶装置１１０３上に格納されているファイルＢ１内のヘッダ情報７０１から、暗号プロトコル変換サーバのサーバ識別子（ここでは、暗号プロトコル変換サーバ１（３０Ａ）のサーバ識別子）７０１２を読み出して、ワークエリア１２０５に設定する（ステップ１３０１）。

【０１０１】続いて、ステップ１３０１でワークエリア１２０５に設定した暗号プロトコル変換サーバのサーバ識別子（ここでは，暗号プロトコル変換サーバ１（３０Ａ）のサーバ識別子）に基づいて、経由された暗号プロ

トコル変換サーバ（ここでは、暗号プロトコル変換サーバ1（30A））を判断する（ステップ1302）。

【0102】続いて、2次記憶装置1103上に格納されているファイルB2内のヘッダ情報702から、暗号プロトコル変換サーバのサーバ識別子（ここでは、暗号プロトコル変換サーバ2（30B）のサーバ識別子）7020を読み出して、ワークエリア1205に設定する（ステップ1303）。

【0103】続いて、ステップ1303でワークエリア1205に設定した暗号プロトコル変換サーバのサーバ識別子（ここでは、暗号プロトコル変換サーバ2（30B）のサーバ識別子）に基づいて、経由された暗号プロトコル変換サーバ（ここでは、暗号プロトコル変換サーバ2（30B））を判断する（ステップ1304）。

【0104】続いて、C2復号化プログラム1202のパラメータとなる、暗号プロトコル変換サーバ1（30A）との間の暗号通信用の鍵KAB1（1206）および暗号用初期値B1（1207）をワークエリア1205に設定する（ステップ1305）。

【0105】続いて、C2復号化プログラム1202のパラメータとなる、暗号プロトコル変換サーバ2（30B）との間の暗号通信用の鍵KBB1（1208）および暗号用初期値B2（1209）をワークエリア1205に設定する（ステップ1306）。

【0106】続いて、2次記憶装置1103上のファイルB1に格納されている再暗号化データを、ワークエリア1205にロードし（ステップ1307）、2次記憶装置1103上のファイルB2に格納されている再暗号化データを、ワークエリア1205にロードする（ステップ1308）。なお、ステップ1307でロードする再暗号化データのデータ量と、ステップ1308でロードする再暗号化データのデータ量とは、同量である。

【0107】続いて、ステップ1305で設定したパラメータをC2復号化プログラム1202に与えて、C2復号化プログラム1202を実行し、ステップ1307でロードした再暗号化データを復号化する（ステップ1309）。

【0108】続いて、ステップ1306で設定したパラメータをC2復号化プログラム1202に与えて、C2復号化プログラム1202を実行し、ステップ1308でロードした再暗号化データを復号化する（ステップ1310）。

【0109】続いて、復元プログラム1204を用いて、ステップ1309およびステップ1310で復号化した2個のデータを、元のデータに復元するための復元処理を行う（ステップ1311）。

【0110】ここで、復元プログラム1204による復元方法の具体例について、図14を用いて説明する。

【0111】図14に示す例では、図5に示した振り分け方法に呼応して、暗号プロトコル変換サーバ1（30A）を経由して受信したデータaと、暗号プロトコル変換サーバ2（30B）を経由して受信したデータbとの間で排他的論理和を先頭から順に取ることにより、データa，bを、元のデータdに復元している。

【0112】さて、図13に戻って、端末10B－1は、復元処理により復元されたデータ（平文）を、2次記憶装置1103上のファイルBに格納する（ステップ1312）。

【0113】続いて、ファイルB1，B2内に未復号化データが格納されているか否かを判定し（ステップ1313）、格納されているならば、ステップ1307～ステップ1312を繰り返す。

【0114】以上説明した動作により、送信先の端末10B－1において、ファイルB内に、送信元の端末10A－1が作成したデータが、判別可能な元の形式（平文）で格納されることとなり、端末10A－1から端末10B－1に対する暗号通信が完了した。

【0115】従って、本実施例の暗号通信システムによれば、暗号プロトコル変換サーバ1（30A），暗号プロトコル変換サーバ2（30B）が、各々、分担して暗号変換処理を行うと共に、分担させるデータの振り分け方法に工夫を施しているので、振り分け方法が明らかになった場合で、かつ、暗号変換処理時の平文が、2個の暗号プロトコル変換サーバ1（30A），暗号プロトコル変換サーバ2（30B）から同時に洩れた場合でない限り、端末10A－1が作成した元のデータ（平文）が第三者に盗まれることはなく、元のデータの盗難を困難にすることができる。

【0116】また、本実施例の暗号通信システムによれば、暗号プロトコル変換サーバ1（30A），暗号プロトコル変換サーバ2（30B）が、各々、暗号変換処理において、1ブロックごとに、復号化および再暗号化を行っているので、同時に平文状態となるデータの量が1ブロックのみであることから、データが平文状態となる時間が短くなる。従って、平文状態のデータが洩れる可能性がある時間が短くなり、また、この時間に平文状態のデータが盗まれても、1ブロック分のデータのみが判明するだけで済む。一方、暗号変換処理において、全てのデータを復号化して平文状態のデータに戻した後、再暗号化する場合を考えてみると、データが平文状態となる時間が長くなるので、平文状態のデータが漏れる可能性がある時間が長くなり、この時間に平文状態のデータが盗まれると、より大量のデータが判明してしまう。

【0117】このように、暗号変換処理において、1ブロックずつ、復号化および再暗号化を行うことで、データが平文状態となる時間が短くなるので、安全性を増加させることができる。

【0118】なお、図1に示した例では、暗号プロトコル変換サーバ1（30A），暗号プロトコル変換サーバ2（30B）が、各々、第三機関AのLAN120A，

第三機関BのLAN120Bに接続されるようにすることで、秘匿性がさらに増加するようにしているが、暗号プロトコル変換サーバ1（30A），暗号プロトコル変換サーバ2（30B）が、共に、WAN110に接続されるようにしてもよい。

【0119】また、以下に示すような様々な変形例も考えられる。

【0120】（変形例1）変形例1は、振り分け方法を、図5に示した振り分け方法の代わりに、図18に示す振り分け方法とした例である。

【0121】図18に示す振り分け方法は、元のデータdの先頭から、1ブロックずつ交互に抽出することにより、暗号プロトコル変換サーバ1（30A）に送信するデータa，および、暗号プロトコル変換サーバ2（30B）に送信するデータbを生成するという方法である。

【0122】なお、復元方法は、データa，bを各々復号化した後、各データの先頭から1ブロックずつ交互に抽出し、連結すればよい。

【0123】図18に示した振り分け方法で生成した2個のデータa，bは、元のデータdの1／2のデータ量であるので、暗号プロトコル変換サーバ1（30A），暗号プロトコル変換サーバ2（30B）間で負荷が分散されることとなる。

【0124】このように、暗号プロトコル変換サーバ1（30A），暗号プロトコル変換サーバ2（30B）に振り分けるデータa，bの量が、元のデータdの量より小さくなると、暗号変換処理に関する負荷分散効果があり、従って、暗号変換処理が高速化されるという効果があるので、特に、大容量の暗号通信に有効となる。

【0125】ただし、図18に示した振り分け方法では、元のデータdに対するブロック単位での転置が行われるので、暗号変換処理時に、再暗号化前の平文状態のデータが、ブロック単位で意味のあるデータとなる。そこで、ブロック長を十分に短くし、ブロック単位での意味が判別困難になるようにすることが好ましい。ブロック長としては、例えば、慣用暗号の1ブロック長（64ビット）や、16ビット未満や、8ビット未満とすることができる。16ビットは、1文字分の漢字コードに相当しているので、16ビット未満とすることで、意味判別が困難になる。また、8ビットは、1文字分の英数字コードに相当しているので、8ビット未満とすることで、意味判別が困難になる。

【0126】このように、ブロック長を十分に短くすると、暗号変換処理時に、平文状態のデータの意味判別が困難になり、安全性を増加させることができる。

【0127】（変形例2）変形例2は、変形例1において、意味判別をさらに困難にするために、図18に示した振り分け方法による振り分けを行う前に、元のデータdの各ブロックを、ランダムに転置しておくものである。

【0128】例えば、元のデータdのブロック数がn個であるとすると、（n！－1）通りの転置方法が存在するので、できるだけランダムな転置を行うために、乱数表を使用するようにし、送信元の端末と送信先の端末とが、同じ乱数表を保持すればよい。

【0129】（変形例3）図1に示した例は、2個の暗号プロトコル変換サーバが接続されているようにしているが、変形例3は、3個以上の暗号プロトコル変換サーバが接続されているようにするものである。

【0130】例えば、3個の暗号プロトコル変換サーバが接続されている場合は、図5に示した振り分け方法で生成した2個のデータa，bを、ほぼ均等に、3個の暗号プロトコル変換サーバに振り分けるようにすればよい。すなわち、例えば、データaの先頭から2／3，データaの残りの1／3およびデータbの先頭から1／3，データbの残りの2／3を、各々、3個の暗号プロトコル変換サーバに振り分ければよい。

【0131】図5に示した振り分け方法で生成した2個のデータa，bは、元のデータdの2倍のデータ量であるので、3個以上の暗号プロトコル変換サーバが接続されている場合には、これらの暗号プロトコル変換サーバ間で負荷が分散されることとなる。

【0132】（変形例4）変形例4は、変形例1において、3個以上の暗号プロトコル変換サーバが接続されているようにするものである。

【0133】例えば、3個の暗号プロトコル変換サーバが接続されている場合は、図18に示した振り分け方法で、元のデータdの先頭から、1ブロックずつ交互に抽出することにより、3個の暗号プロトコル変換サーバに各々送信する3個のデータを生成すればよい。

【0134】なお、図18に示した振り分け方法では、k個（≧3）の暗号プロトコル変換サーバが接続されている場合には、k個の暗号プロトコル変換サーバに各々送信されるk個のデータが生成され、これらk個のデータは、元のデータdの1／kのデータ量であるので、これらk個の暗号プロトコル変換サーバ間で負荷が分散されることとなる。

【0135】（変形例5）変形例5は、図5に示した振り分け方法で、元のデータdからデータa，bを生成した後、さらに、同じ振り分け方法で、データaからデータa1，a2を生成し、データbからデータb1，b2を生成するようするものである。

【0136】この場合、例えば、暗号プロトコル変換サーバA（30A）には、データa1，b1を振り分け，暗号プロトコル変換サーバB（30B）には、データa2，b2を振り分けるようにすればよい。

【0137】この場合には、暗号変換処理に関する負荷分散効果はなく、むしろ負荷が2倍に増大してしまう。しかしながら、4個の暗号プロトコル変換サーバが接続されているようにすれば、負荷の増大を解消することが

でき、また、５個以上の暗号プロトコル変換サーバが接続されているようにすれば、負荷を分散させることができる。

【０１３８】（変形例６）図１に示した例は、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１～１０Ａ－ｍ、および、ＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１～１０Ｂ－ｎが、同ブロック長のブロック型慣用暗号を使用するものとしているが、変形例６は、ストリーム暗号または公開鍵暗号を使用するようにするものである。

【０１３９】ブロック型慣用暗号が、数十ビット以上の比較的長いデータブロックごとに暗号化／復号化する暗号であるのに対して、慣用暗号の一種であるストリーム暗号は、１ビットから数ビットの小データブロックごとに暗号化／復号化する暗号である。例えば、ブロック型慣用暗号のうちのＤＥＳ（Data Encryption Standard）暗号は、６４ビットごとに暗号化／復号化する暗号であり、ブロック型慣用暗号のうちのＭｕｌｔｉ２（Multi-Media Encryption Algorithm2）暗号は、６４ビットごとに暗号化／復号化する暗号であり、ストリーム暗号のうちのバーナム暗号は、１ビットごとに暗号化／復号化する暗号である。

【０１４０】また、公開鍵暗号は、相当長いデータブロックごとに暗号化／復号化する暗号である。例えば、公開鍵暗号のうちのＲＳＡ暗号は、６４バイト（＝５１２ビット）ごとに暗号化／復号化する暗号である。

【０１４１】なお、ＤＥＳ暗号の詳細については、「現代暗号理論」（電子通信学会）の４１頁～４９頁に記載されており、ＲＳＡ暗号の詳細については、「現代暗号理論」（電子通信学会）の１０５頁～１２３頁に記載されている。また、Ｍｕｌｔｉ２暗号の詳細については、「マルチメディア向け高速暗号アルゴリズムHisecurity-Multi2の開発と利用法」（電子通信学会，暗号と情報セキュリティジョイントワークショップ講演論文集）の１６７頁～１７３頁に記載されている。

【０１４２】例えば、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１～１０Ａ－ｍが、バーナム暗号を使用し、ＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１～１０Ｂ－ｎが、ＤＥＳ暗号を使用している場合は、暗号変換処理において、バーナム暗号で１ビットずつ６４ビットを復号化する度に、ＤＥＳ暗号で該６４ビットを再暗号化すればよい。

【０１４３】また、例えば、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１～１０Ａ－ｍが、ＲＳＡ暗号を使用し、ＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１～１０Ｂ－ｎが、ＤＥＳ暗号を使用している場合は、暗号変換処理において、ＲＳＡ暗号で６４バイトを復号化する度に、ＤＥＳ暗号で該６４バイトを６４ビットずつ再暗号化すればよい。

【０１４４】また、例えば、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１～１０Ａ－ｍが、ＲＳＡ暗号を使用し、ＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１～１０Ｂ－ｎが、バーナム暗号を使用している場合は、暗号変換処理において、ＲＳＡ暗号で６４バイトを復号化する度に、バーナム暗号で該６４バイトを１ビットずつ再暗号化すればよい。

【０１４５】ところで、互いに異なる暗号を使用する異国の端末間で暗号通信を行いたい場合に、少なくとも一方の国が、法律的に暗号技術に関する輸出入規制を行っており、輸出規制を行っている国の端末で使用している暗号のアルゴリズムを、他国の暗号プロトコル変換サーバに備えることができないという状況が考えられる。例えば、上述した暗号プロトコル変換サーバ１（３０Ａ），暗号プロトコル変換サーバ２（３０Ｂ）の少なくとも一方が、輸出規制国外にある場合は、そのような暗号プロトコル変換サーバに、輸出規制国の端末で使用している暗号のアルゴリズムを備えることができない。

【０１４６】そこで、このような状況において、２国の端末間で暗号通信を行うことを可能とするためには、一般に、特定の１個の暗号のみを共通に使用することを、２国間で協定する方法が考えられる。このように、２国間で共通に使用される暗号を「中間暗号」と呼ぶ。

【０１４７】そこで、中間暗号の使用を協定した場合の実施例を、第２の実施例として、以下に説明する。

【０１４８】図１５は第２の実施例の暗号通信システムの構成図である。

【０１４９】図１５に示した暗号通信システムは、Ａ国に属し、Ａ国で使用されている暗号を使用するＬＡＮ－Ａ（１００Ａ）と、Ｂ国に属し、Ｂ国で使用されている暗号を使用するＬＡＮ－Ｂ（１００Ｂ）に各々接続されている任意の端末間で、暗号通信を行うためのものである。

【０１５０】この暗号通信は、Ａ国に属する、ＷＡＮ－Ａ（１１０Ａ），暗号プロトコル変換サーバＡ１（４０Ａ－１），暗号プロトコル変換サーバＡ２（４０Ａ－２）と、Ｂ国に属する、ＷＡＮ－Ｂ（１１０Ｂ），暗号プロトコル変換サーバＢ１（４０Ｂ－１），暗号プロトコル変換サーバＢ２（４０Ｂ－２）を経由して行われる。

【０１５１】図１５に示すように、ＬＡＮ－Ａ（１００Ａ）は、複数の端末１０Ａ－１～１０Ａ－ｍが接続されたローカルエリア・ネットワークであり、通信回線５０を介して、Ａ国内のＷＡＮ－Ａ（１１０Ａ）と接続されている。また、ＬＡＮ－Ｂ（１００Ｂ）は、複数の端末１０Ｂ－１～１０Ｂ－ｎが接続されたローカルエリア・ネットワークであり、通信回線５２を介して、Ｂ国内のＷＡＮ－Ｂ（１１０Ｂ）と接続されている。また、Ａ国内のＷＡＮ－Ａ（１１０Ａ）とＢ国内のＷＡＮ－Ｂ（１１０Ｂ）とが、通信回線５１を介して接続されている。

【０１５２】Ａ国内には、暗号プロトコル変換サーバＡ

1（40A－1），暗号プロトコル変換サーバA2（40A－2）が設置されており、各々、暗号アルゴリズムC1および中間暗号の暗号アルゴリズムを備えている。また、暗号プロトコル変換サーバA1（40A－1），暗号プロトコル変換サーバA2（40A－2）は、各々、第三機関A1のLAN（130A－1），第三機関A2のLAN（130A－2）に属し、LAN（130A－1），LAN（130A－2）は、各々、通信回線53，54を介して、WAN－A（110A）と接続されている。

【0153】また、B国内には、暗号プロトコル変換サーバB1（40B－1），暗号プロトコル変換サーバB2（40B－2）が設置されており、各々、暗号のアルゴリズムC2および中間暗号のアルゴリズムを備えている。また、暗号プロトコル変換サーバB1（40B－1），暗号プロトコル変換サーバB2（40B－2）は、各々、第三機関B1のLAN（130B－1），第三機関B2のLAN（130B－2）に属し、LAN（130B－1），LAN（130B－2）は、各々、通信回線55，56を介して、WAN－B（110B）と接続されている。

【0154】以下、LAN－A（100A）に接続された端末10A－1からLAN－B（100B）に接続された端末10B－1に対する暗号通信を例にして、上述した暗号通信システムとは異なる点を中心に、暗号通信システムの詳細な動作について説明する。

【0155】端末10A－1のハードウェアの主要部分を示す構成図は、図2と同様であり、端末10B－1のハードウェアの主要部分を示す構成図は、図11と同様である。

【0156】また、端末10A－1の主記憶装置202の利用形態を示す説明図、および、端末10A－1の送信処理手順を示すフローチャートは、実質的には、図3および図4と同様である。

【0157】ただし、端末10A－1においては、上述した暗号通信システムにおける暗号プロトコル変換サーバ1（30A）を暗号プロトコル変換サーバA1（40A－1）とみなし、上述した暗号通信システムにおける暗号プロトコル変換サーバ2（30B）を暗号プロトコル変換サーバA2（40A－2）とみなすようにする。すなわち、端末10A－1は、端末10B－1に送信すべきデータを、暗号プロトコル変換サーバA1（40A－1），暗号プロトコル変換サーバA2（40A－2）の各々に振り分け、暗号化して送信する。

【0158】また、端末10B－1の主記憶装置1102の利用形態を示す説明図、および、端末10B－1の送信処理手順を示すフローチャートは、実質的には、図12および図13と同様である。

【0159】ただし、端末10B－1においては、上述した暗号通信システムにおける暗号プロトコル変換サーバ1（30A）を暗号プロトコル変換サーバB1（40B－1）とみなし、上述した暗号通信システムにおける暗号プロトコル変換サーバ2（30B）を暗号プロトコル変換サーバB2（40B－2）とみなすようにする。すなわち、端末10B－1は、暗号プロトコル変換サーバB1（40B－1），暗号プロトコル変換サーバB2（40B－2）を各々経由して送信されたデータを、復号化して元のデータに復元する。

【0160】また、暗号プロトコル変換サーバA1（40A－1）の構成図，暗号プロトコル変換サーバA2（40A－2）の構成図，暗号プロトコル変換サーバB1（40B－1）の構成図，暗号プロトコル変換サーバB2（40B－2）の構成図は、図8と同様である。

【0161】図16は暗号プロトコル変換サーバA1（40A－1）の主記憶装置802の利用形態を示す説明図である。

【0162】図16に示すように、主記憶装置802上には、LAN－A（100A）で使用されている暗号アルゴリズムC1を用いたC1暗号化プログラム1601およびC1復号化プログラム1602と、中間暗号の暗号アルゴリズムを用いた中間暗号暗号化プログラム1603および中間暗号復号化プログラム1604とが格納され、また、ワークエリア1605が確保されている。

【0163】さらに、暗号通信の送受信時に使用する情報として、端末10A－1～10A－mの各々との間の暗号通信用の鍵が設定されている鍵エリア1606と、暗号プロトコル変換サーバB1（40B－1）との間の暗号通信用の鍵1607と、暗号用初期値A1（1608）とが格納されている。

【0164】実際には、鍵エリア1606には、端末10A－1～10A－mの端末識別子16061ごとに、対応する鍵16062が設定されている。また、暗号用初期値A1（1608）は、端末10A－1の主記憶装置202上に格納されている暗号用初期値A1（307）と同じ値である。

【0165】なお、暗号プロトコル変換サーバA2（40A－2）の主記憶装置802の利用形態を示す説明図も、図16と同様である。ただし、暗号プロトコル変換サーバB1（40B－1）との間の暗号通信用の鍵の代わりに、暗号プロトコル変換サーバB2（40B－2）との間の暗号通信用の鍵が格納されている。

【0166】図17は暗号プロトコル変換サーバB1（40B－1）の主記憶装置802の利用形態を示す説明図である。

【0167】図17に示すように、主記憶装置802上には、LAN－B（100B）で使用されている暗号アルゴリズムC2を用いたC2暗号化プログラム1701およびC2復号化プログラム1702と、中間暗号の暗号アルゴリズムを用いた中間暗号暗号化プログラム1703および中間暗号復号化プログラム1704とが格納

され、また、ワークエリア１７０５が確保されている。

【０１６８】さらに、暗号通信の送受信時に使用する情報として、端末１０Ｂ－１～１０Ｂ－ｎの各々との間の暗号通信用の鍵が設定されている鍵エリア１７０６と、暗号プロトコル変換サーバＡ１（４０Ａ－１）との間の暗号通信用の鍵１７０７と、暗号用初期値Ｂ１（１７０８）とが格納されている。

【０１６９】実際には、鍵エリア１７０６には、端末１０Ｂ－１～１０Ｂ－ｎの端末識別子１７０６１ごとに、対応する鍵１７０６２が設定されている。また、暗号用初期値Ｂ１（１７０８）は、端末１０Ｂ－１の主記憶装置１１０２上に格納されている暗号用初期値Ｂ１（１１０７）と同じ値である。

【０１７０】なお、暗号プロトコル変換サーバＢ２（４０Ｂ－２）の主記憶装置８０１の利用形態を示す説明図も、図１７と同様である。ただし、暗号プロトコル変換サーバＡ１（４０Ａ－１）との間の暗号通信用の鍵の代わりに、暗号プロトコル変換サーバＡ２（４０Ａ－２）との間の暗号通信用の鍵が格納されている。

【０１７１】また、暗号プロトコル変換サーバＡ１（４０Ａ－１），暗号プロトコル変換サーバＡ２（４０Ａ－２）の暗号変換処理手順は、実質的には、図１０と同様である。

【０１７２】ただし、暗号プロトコル変換サーバＡ１（４０Ａ－１），暗号プロトコル変換サーバＡ２（４０Ａ－２）は、暗号変換処理において、Ｃ１復号化プログラム９０２による復号化を行い、Ｃ２暗号化プログラム９０３による再暗号化を行う代わりに、Ｃ１復号化プログラム１６０２による復号化を行い、中間暗号暗号化プログラム１６０３による再暗号化を行うようにする。また、暗号プロトコル変換サーバＡ１（４０Ａ－１）は、再暗号化データを格納したファイルを、暗号プロトコル変換サーバＢ１（４０Ｂ－１）に送信するようにし、暗号プロトコル変換サーバＡ２（４０Ａ－２）は、再暗号化データを格納したファイルを、暗号プロトコル変換サーバＢ２（４０Ｂ－２）に送信するようにする。

【０１７３】なお、ここでは、暗号プロトコル変換サーバＡ１（４０Ａ－１）と暗号プロトコル変換サーバＢ１（４０Ｂ－１）との間で中間暗号を使用した暗号通信を行い、暗号プロトコル変換サーバＡ２（４０Ａ－２）と暗号プロトコル変換サーバＢ２（４０Ｂ－２）との間で中間暗号を使用した暗号通信を行うようにしているが、１個の暗号プロトコル変換サーバに重複して送信されないようになっていればよい。

【０１７４】また、暗号プロトコル変換サーバＢ１（４０Ｂ－１），暗号プロトコル変換サーバＢ２（４０Ｂ－２）の暗号変換処理手順も、実質的には、図１０と同様である。

【０１７５】ただし、暗号プロトコル変換サーバＢ１（４０Ｂ－１），暗号プロトコル変換サーバＢ２（４０Ｂ－２）は、暗号変換処理において、Ｃ１復号化プログラム９０２による復号化を行い、Ｃ２暗号化プログラム９０３による再暗号化を行う代わりに、中間暗号復号化プログラム１７０４による復号化を行い、Ｃ２暗号化プログラム１７０１による再暗号化を行うようにする。

【０１７６】このように、中間暗号の使用を協定した場合には、暗号プロトコル変換サーバＡ１（４０Ａ－１），暗号プロトコル変換サーバＡ２（４０Ａ－２）は、各々、暗号プロトコル変換サーバＢ１（４０Ｂ－１），暗号プロトコル変換サーバＢ２（４０Ｂ－２）との間の暗号通信用の鍵１６０７、および、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１～１０Ａ－ｍの各々との間の暗号通信用の鍵１６０６２を保持していればよく、ＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１～１０Ｂ－ｎの各々との間の暗号通信用の鍵１７０６２を保持する必要はない。また、暗号プロトコル変換サーバＢ１（４０Ｂ－１），暗号プロトコル変換サーバＢ２（４０Ｂ－２）も、各々、暗号プロトコル変換サーバＡ１（４０Ａ－１），暗号プロトコル変換サーバＡ２（４０Ａ－２）との間の暗号通信用の鍵１７０７、および、ＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１～１０Ｂ－ｎの各々との間の暗号通信用の鍵１７０６２を保持していればよく、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１～１０Ａ－ｍの各々との間の暗号通信用の鍵１６０６２を保持する必要はない。

【０１７７】従って、自国で使用している暗号のアルゴリズムを他国に属する暗号プロトコル変換サーバに備えなくても、暗号通信を行うことができる。

【０１７８】なお、図１５に示した例では、暗号プロトコル変換サーバＡ１（４０Ａ－１），暗号プロトコル変換サーバＡ２（４０Ａ－２）が、各々、第三機関Ａ１のＬＡＮ（１３０Ａ－１），第三機関Ａ２のＬＡＮ（１３０Ａ－２）に接続されるようにし、暗号プロトコル変換サーバＢ１（４０Ｂ－１），暗号プロトコル変換サーバＢ２（４０Ｂ－２）が、各々、第三機関Ｂ１のＬＡＮ（１３０Ｂ－１），第三機関Ｂ２のＬＡＮ（１３０Ｂ－２）に接続されるようにすることで、秘匿性がさらに増加するようにしているが、暗号プロトコル変換サーバＡ１（４０Ａ－１），暗号プロトコル変換サーバＡ２（４０Ａ－２）が、共に、ＷＡＮ－Ａ（１１０Ａ）に接続されるようにし、暗号プロトコル変換サーバＢ１（４０Ｂ－１），暗号プロトコル変換サーバＢ２（４０Ｂ－２）が、共に、ＷＡＮ－Ｂ（１１０Ｂ）に接続されるようにしてもよい。

【０１７９】なお、中間暗号の使用を協定した場合でも、上述と同様な変形例が考えられる。

【０１８０】すなわち、上述した変形例１と同様に、振り分け方法を、図５に示した振り分け方法の代わりに、図１８に示す振り分け方法とすることができる。

【０１８１】また、上述した変形例２と同様に、図１８

に示した振り分け方法による振り分けを行う前に、元のデータｄの各ブロックを、ランダムに転置しておくことができる。

【０１８２】また、上述した変形例３と同様に、Ａ国に属する暗号プロトコル変換サーバ、および、Ｂ国に属する暗号プロトコル変換サーバが、各々、３個以上接続されているようにすることができる。

【０１８３】また、上述した変形例４と同様に、変形例１においても、Ａ国に属する暗号プロトコル変換サーバ、および、Ｂ国に属する暗号プロトコル変換サーバが、各々、３個以上接続されているようにすることができる。

【０１８４】また、上述した変形例５と同様に、図５に示した振り分け方法で、元のデータｄからデータａ，ｂを生成した後、さらに、同じ振り分け方法で、データａからデータａ１，ａ２を生成し、データｂからデータｂ１，ｂ２を生成するようにすることができる。

【０１８５】また、上述した変形例６と同様に、ＬＡＮ－Ａ（１００Ａ）に接続された端末１０Ａ－１～１０Ａ－ｍ、および、ＬＡＮ－Ｂ（１００Ｂ）に接続された端末１０Ｂ－１～１０Ｂ－ｎが、ストリーム暗号または公開鍵暗号を使用するようにすることができる。

【０１８６】

【発明の効果】以上説明したように、本発明の暗号通信システムにおいては、送信元の端末が、送信すべきデータから、平文状態で意味判別困難な複数のデータを生成し、生成した複数のデータを暗号化してから複数の暗号プロトコル変換サーバに振り分けて送信するようにしているので、複数の暗号プロトコル変換サーバが暗号変換処理を分担して行うようにすることができ、さらに、各暗号プロトコル変換サーバが、一定のデータ量ごとに暗号変換処理を行うようにすることもできるので、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、安全に行うことが可能となる。

【０１８７】また、送信元の端末が、送信すべきデータから、該データのデータ量よりデータ量が小さい複数のデータを生成するようにすれば、複数の暗号プロトコル変換サーバ間で負荷が分散され、各暗号プロトコル変換サーバが行う暗号変換処理の負荷が軽減されるので、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、高速に行うことが可能となる。

【０１８８】さらに、互いに異なる暗号を使用する端末が異なる国に属する場合でも、これらの国が共通に使用するよう協定した１個の暗号を利用し、これらの端末間で送受信されるデータが、国境を越えるときに、該協定した暗号で暗号化された状態となるようにすれば、互いに異なる暗号を使用する端末間で暗号通信を行う際の暗号変換処理を、安全に行うことが可能となる。

【図面の簡単な説明】

【図１】第１の実施例の暗号通信システムの構成図。

【図２】送信元の端末のハードウェアの主要部分を示す構成図。

【図３】送信元の端末の主記憶装置の利用形態を示す説明図。

【図４】送信元の端末の送信処理手順を示すフローチャート。

【図５】振り分けプログラムによる振り分け方法の具体例を示す説明図。

【図６】ＣＢＣモードでの暗号化を示す説明図。

【図７】ヘッダ情報の形式を示す説明図。

【図８】暗号プロトコル変換サーバのハードウェアの主要部分を示す構成図。

【図９】暗号プロトコル変換サーバの主記憶装置の利用形態を示す説明図。

【図１０】暗号プロトコル変換サーバの暗号変換処理手順を示すフローチャート。

【図１１】送信先の端末のハードウェアの主要部分を示す構成図。

【図１２】送信先の端末の主記憶装置の利用形態を示す説明図。

【図１３】送信先の端末の受信処理手順を示すフローチャート。

【図１４】復元プログラムによる復元方法の具体例を示す説明図。

【図１５】第２の実施例の暗号通信システムの構成図。

【図１６】Ａ国内の暗号プロトコル変換サーバの主記憶装置の利用形態を示す説明図。

【図１７】Ｂ国内の暗号プロトコル変換サーバの主記憶装置の利用形態を示す説明図。

【図１８】振り分けプログラムによる振り分け方法の他の具体例を示す説明図。

【符号の説明】

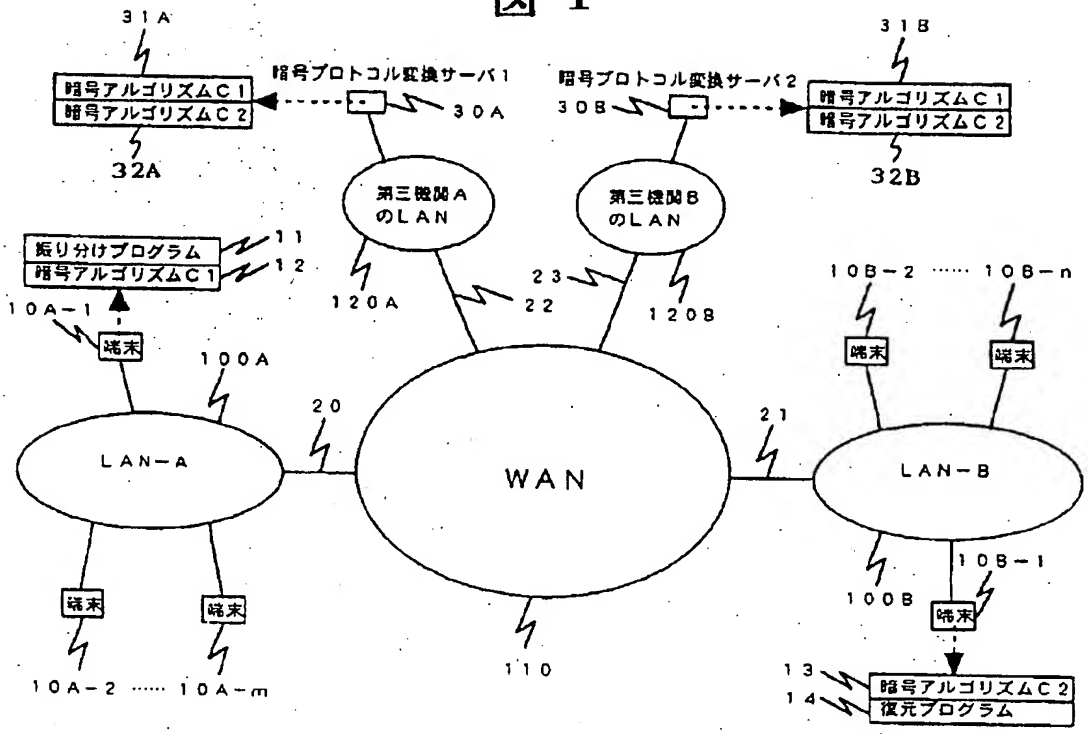
１００Ａ…ＬＡＮ－Ａ、１００Ｂ…ＬＡＮ－Ｂ、１０Ａ－１～１０Ａ－ｍ…ＬＡＮ－Ａに接続された端末、１０Ｂ－１～１０Ｂ－ｎ…ＬＡＮ－Ｂに接続された端末、１１…振り分けプログラム、１２，３１Ａ，３１Ｂ…暗号アルゴリズムＣ１、１３，３２Ａ，３２Ｂ…暗号アルゴリズムＣ２、１４…復元プログラム、３０Ａ…暗号プロトコル変換サーバ１、３０Ｂ…暗号プロトコル変換サーバ２、１１０…ＷＡＮ、１２０Ａ…第三機関ＡのＬＡＮ、１２０Ｂ…第三機関ＢのＬＡＮ、４０Ａ－１，４０Ａ－２…Ａ国内の暗号プロトコル変換サーバ、４０Ｂ－１，４０Ｂ－２…Ｂ国内の暗号プロトコル変換サーバ、１１０Ａ…Ａ国内のＷＡＮ－Ａ、１１０Ｂ…Ｂ国内のＷＡＮ－Ｂ、１３０Ａ－１，１３０Ａ－２…Ａ国内の第三機関のＬＡＮ、１３０Ｂ－１，１３０Ｂ－２…Ｂ国内の第三機関のＬＡＮ、２０１，８０１，１１０１…ＣＰＵ、２０２，８０２，１１０２…主記憶装置、２０３，８０３，１１０３…２次記憶装置、２０４，８０４，１１０４…通信アダプタ、２０５，８０５，１１０５…バ

31　　32

ス。

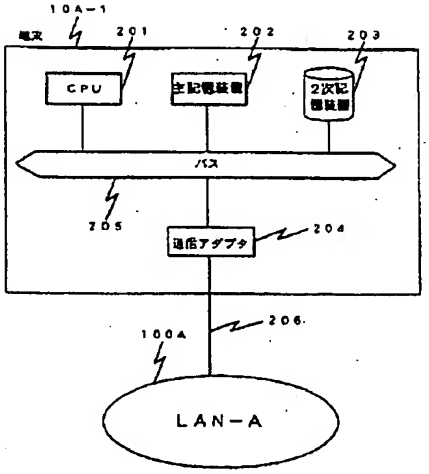
【図１】

図 1



【図２】

図2

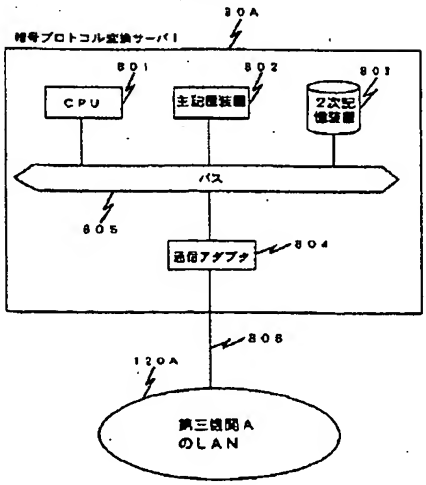


【図３】

図3

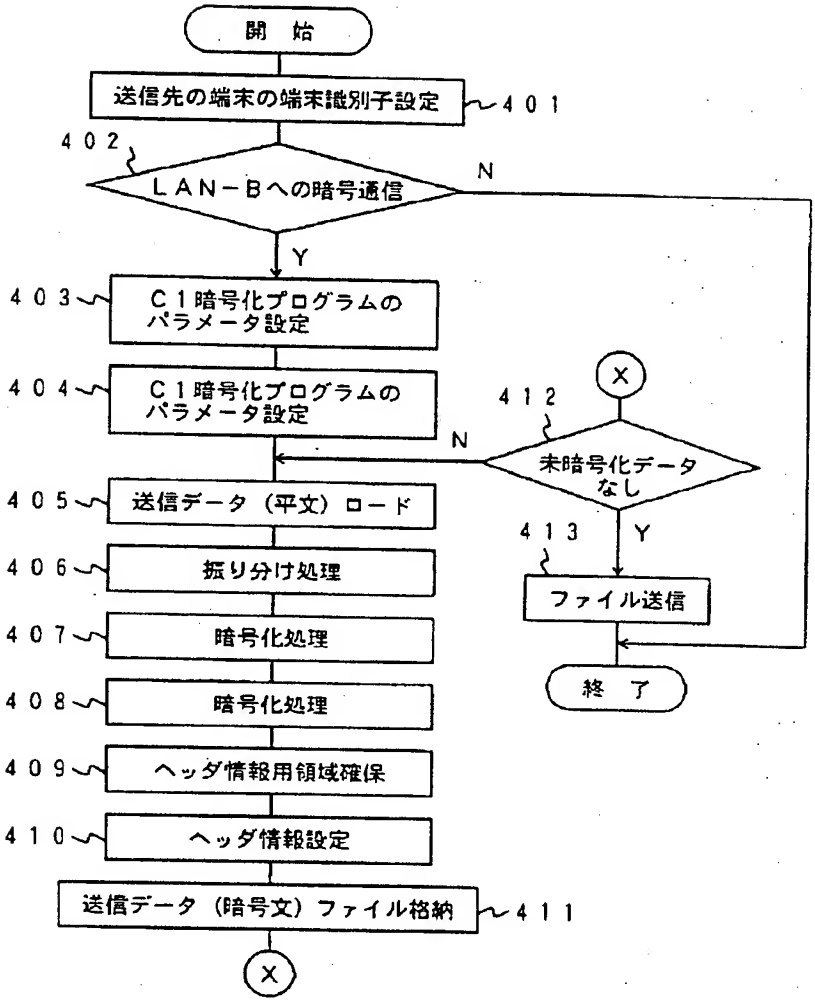
【図８】

図8



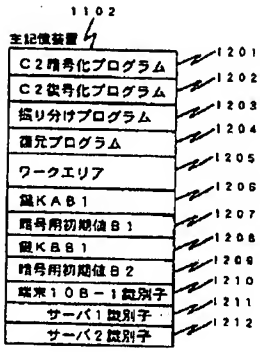
【図4】

図　4


開　始
送信先の端末の端末識別子設定
401
402
LAN－Bへの暗号通信
N
Y
403
C1暗号化プログラムの
パラメータ設定
404
C1暗号化プログラムの
パラメータ設定
X
412
未暗号化データ
なし
N
405
送信データ（平文）ロード
413
Y
406
振り分け処理
ファイル送信
407
暗号化処理
408
暗号化処理
409
ヘッダ情報用領域確保
410
ヘッダ情報設定
送信データ（暗号文）ファイル格納
411
X
終　了

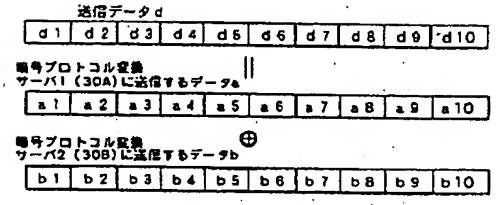
【図12】

図12


1102
主記憶装置
C2暗号化プログラム
1201
C2復号化プログラム
1202
振り分けプログラム
1203
復元プログラム
1204
ワークエリア
1205
鍵KAB1
1206
暗号用初期値B1
1207
鍵KBB1
1208
暗号用初期値B2
1209
端末108－1識別子
1210
サーバ1識別子
1211
サーバ2識別子
1212

【図5】

図5



データa，bの生成方法の例

(1) a1には、任意の乱数を与える

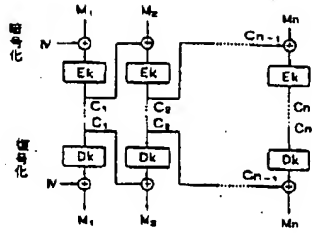
(2) b1 = d1⊕a1

(3) a2 = b1，b2 = d2⊕a2

(4) a(i) = b(i-1)，b(i) = d(i)⊕a(i)　(3=<i<=10)

【図6】

図6



M(i)(1=<i=<n)：平文系列

C(i)(1=<i=<n)：平文系列M(i)に対する暗号文系列

ＩＶ：初期定数

Ek：暗号鍵kを用いた暗号化関数

Dk：暗号鍵kを用いた復号関数

C(1) = Ek(M(1)⊕ＩＶ)

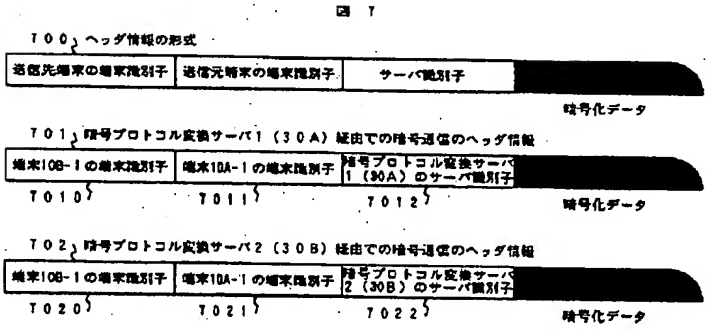
C(i) = Ek(M(i)⊕C(i-1))　(2=<i=<n)

M(1) = Dk(C(1))⊕ＩＶ

M(i) = Dk(C(i))⊕C(i-1)　(2=<i=<n)

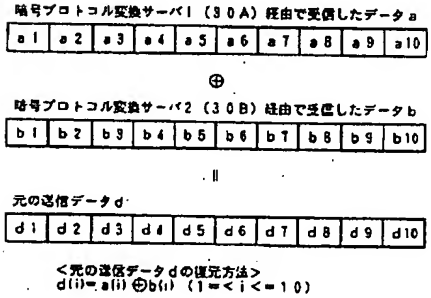
【図7】

図 7



【図14】

図14

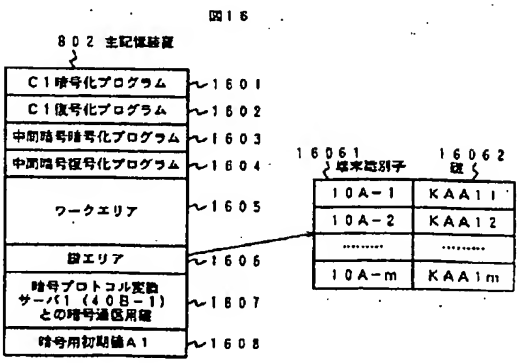


<元の送信データdの復元方法>

d(i)=a(i)⊕b(i)　(1=<i<=10)

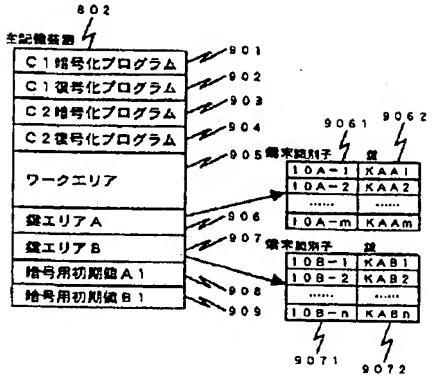
【図16】

図16



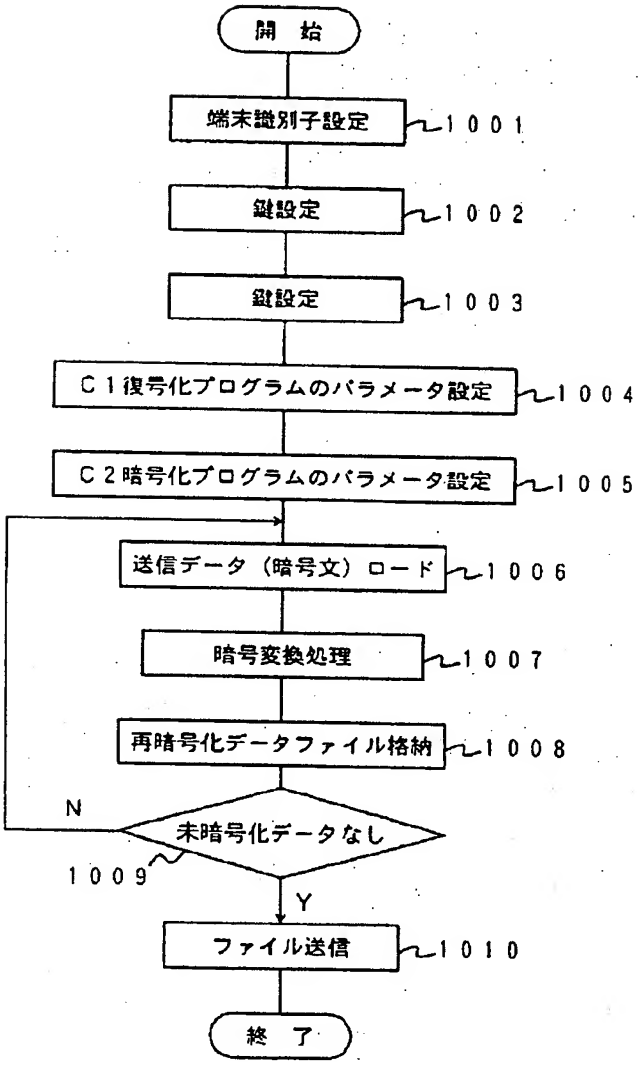
【図９】

図９



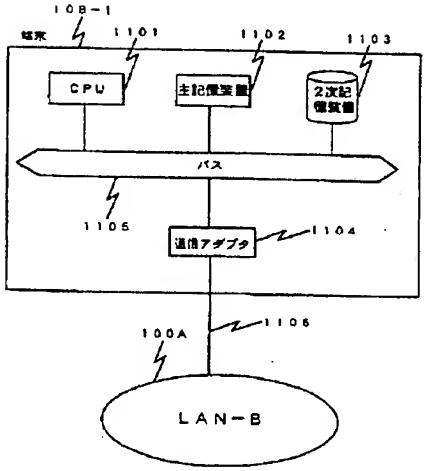
【図１０】

図１０



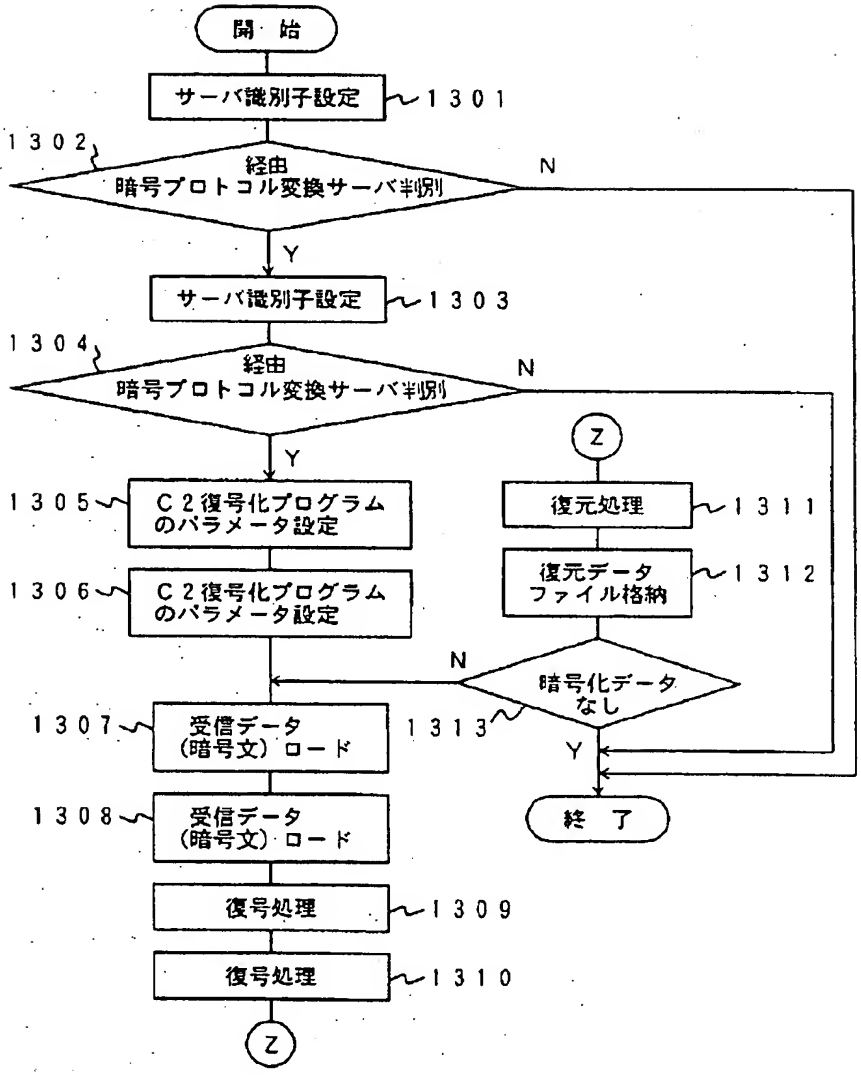
【図１１】

図11



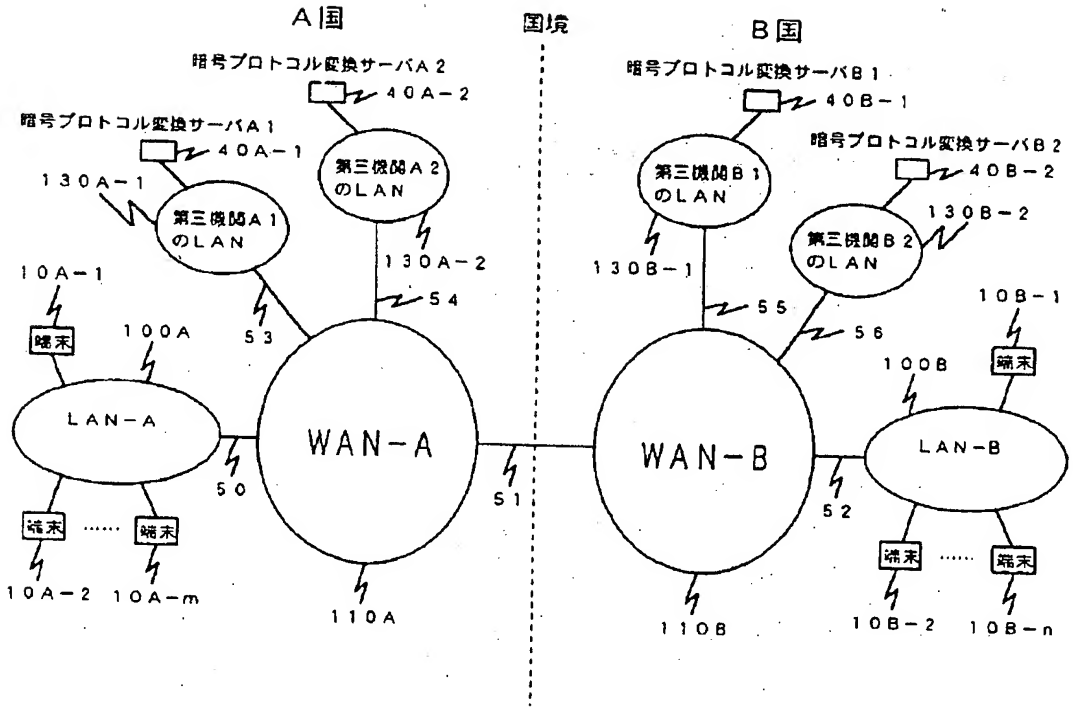
【図13】

図13


開　始
サーバ識別子設定
1301
1302
経由
暗号プロトコル変換サーバ判別
N
Y
サーバ識別子設定
1303
1304
経由
暗号プロトコル変換サーバ判別
N
Y
Z
1305
C2復号化プログラム
のパラメータ設定
1306
C2復号化プログラム
のパラメータ設定
復元処理
1311
復元データ
ファイル格納
1312
N
暗号化データ
なし
1313
1307
受信データ
(暗号文) ロード
Y
1308
受信データ
(暗号文) ロード
終　了
復号処理
1309
復号処理
1310
Z

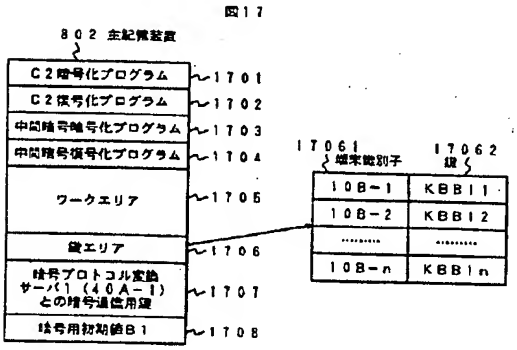
【図15】

図15



【図17】

図17



【図18】

図18